Towards Secure and Dependable Authentication and Authorization Infrastructures

Diego Kreutz, Alysson Bessani, Eduardo Feitosa, Hugo Cunha

PRDC2014, Singapore

Cyber threats: state of affairs

NSA Director Rogers Urges Cyber-Resiliency
Threat Post, Washington, D.C. (United States)

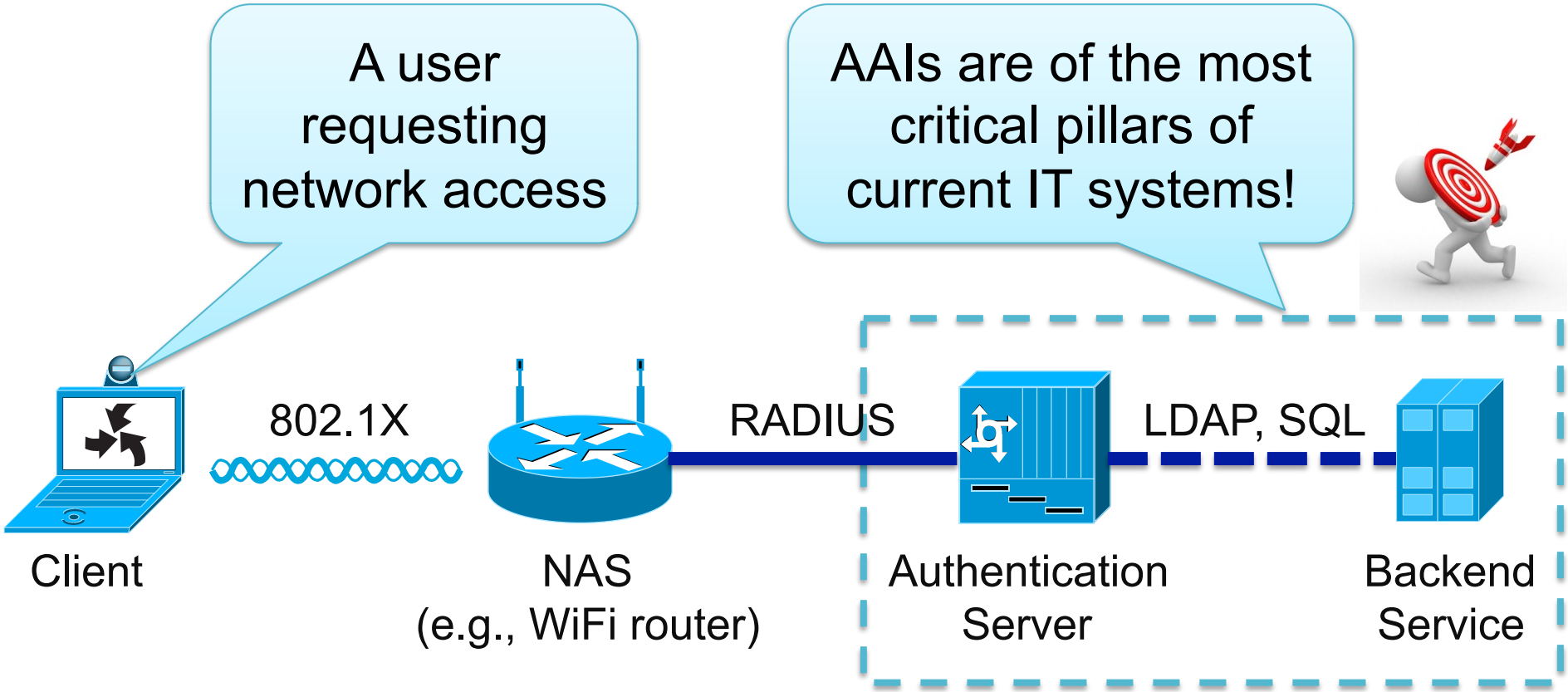
Presidential Proclamation:
Critical Infrastructure Security and Resilience Month, 2014
The White House, Washington, D.C. (United States)

Biggest ever cyber security exercise in Europe today
European Commission - PRESS RELEASES, October 30, 2014

Survey: Cyber security priorities shift to insider threats
FEDERALTIMES US

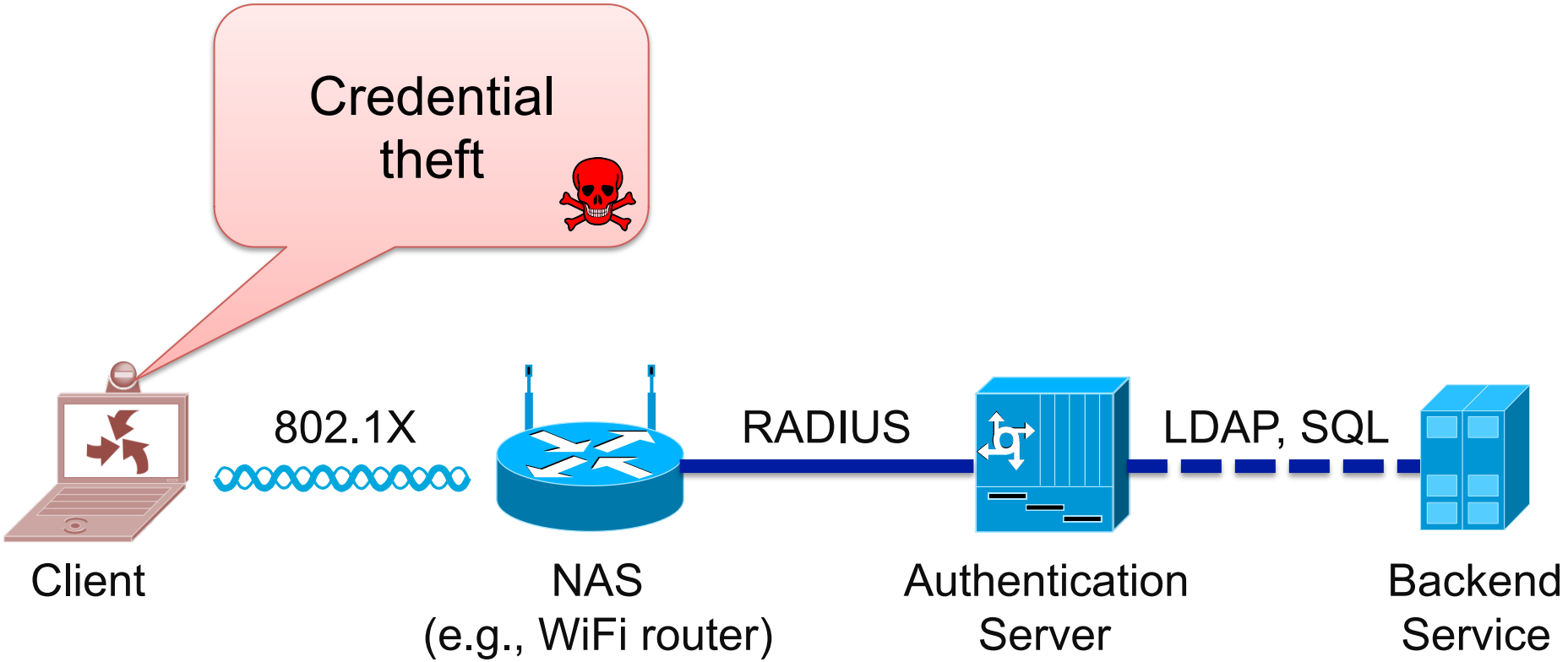
Authentication & Authorization Infra (AAI)

A typical Authentication & Authorization architecture in an enterprise network



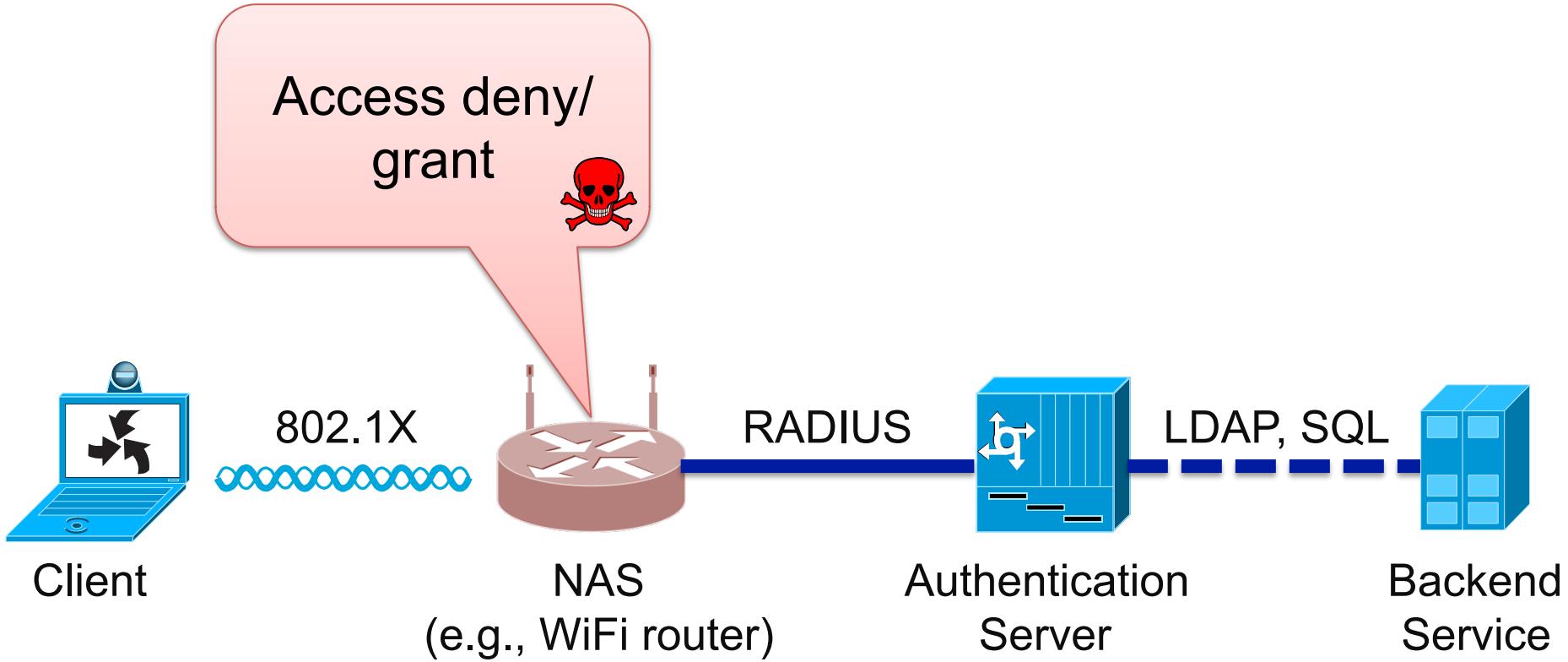
Authentication & Authorization Infra (AAI)

A typical Authentication & Authorization architecture in an enterprise network



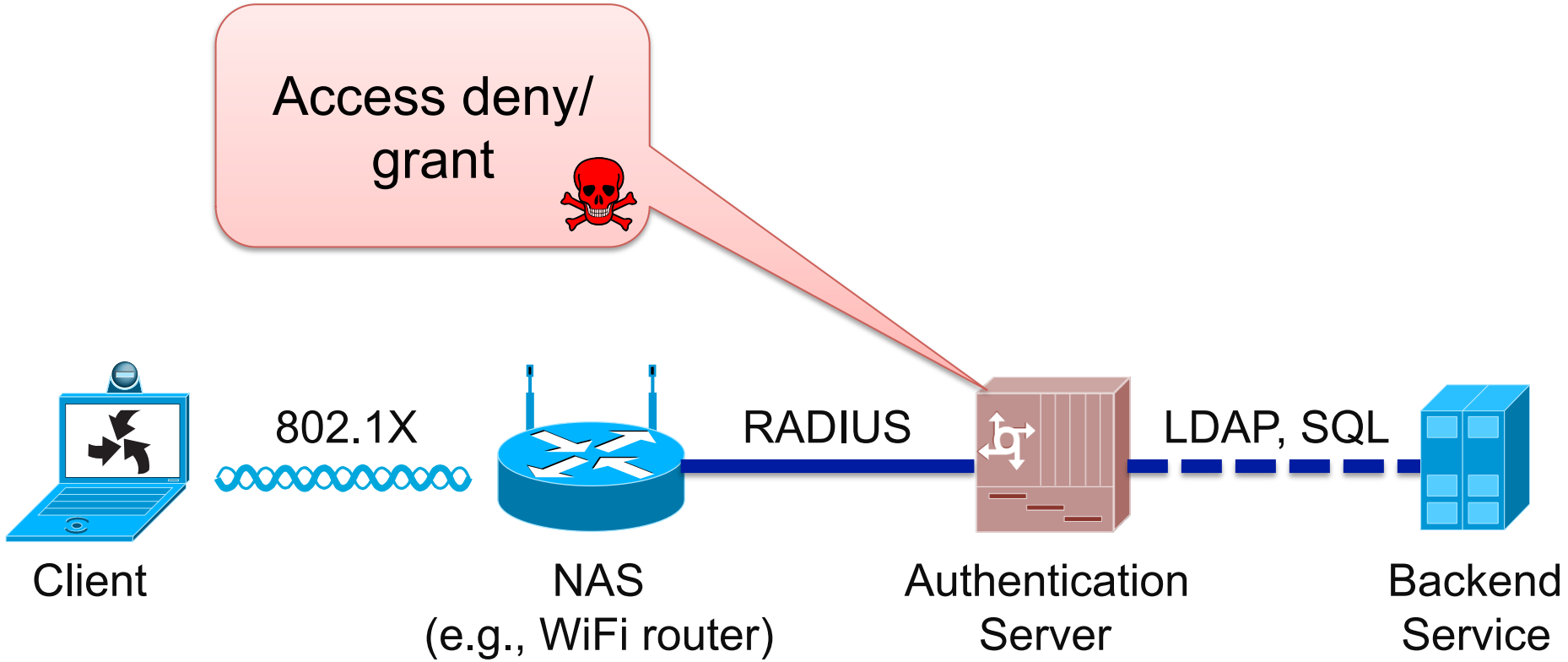
Authentication & Authorization Infra (AAI)

A typical Authentication & Authorization architecture in an enterprise network



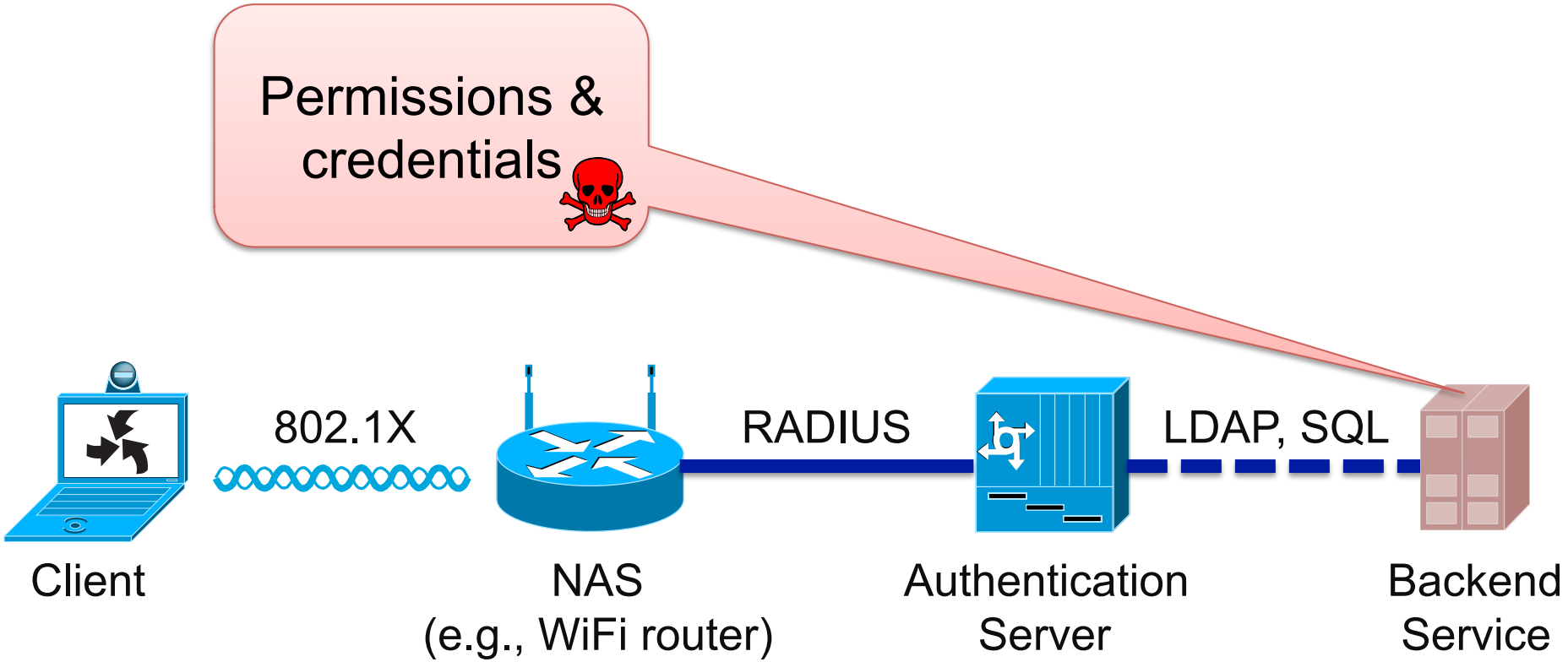
Authentication & Authorization Infra (AAI)

A typical Authentication & Authorization architecture in an enterprise network



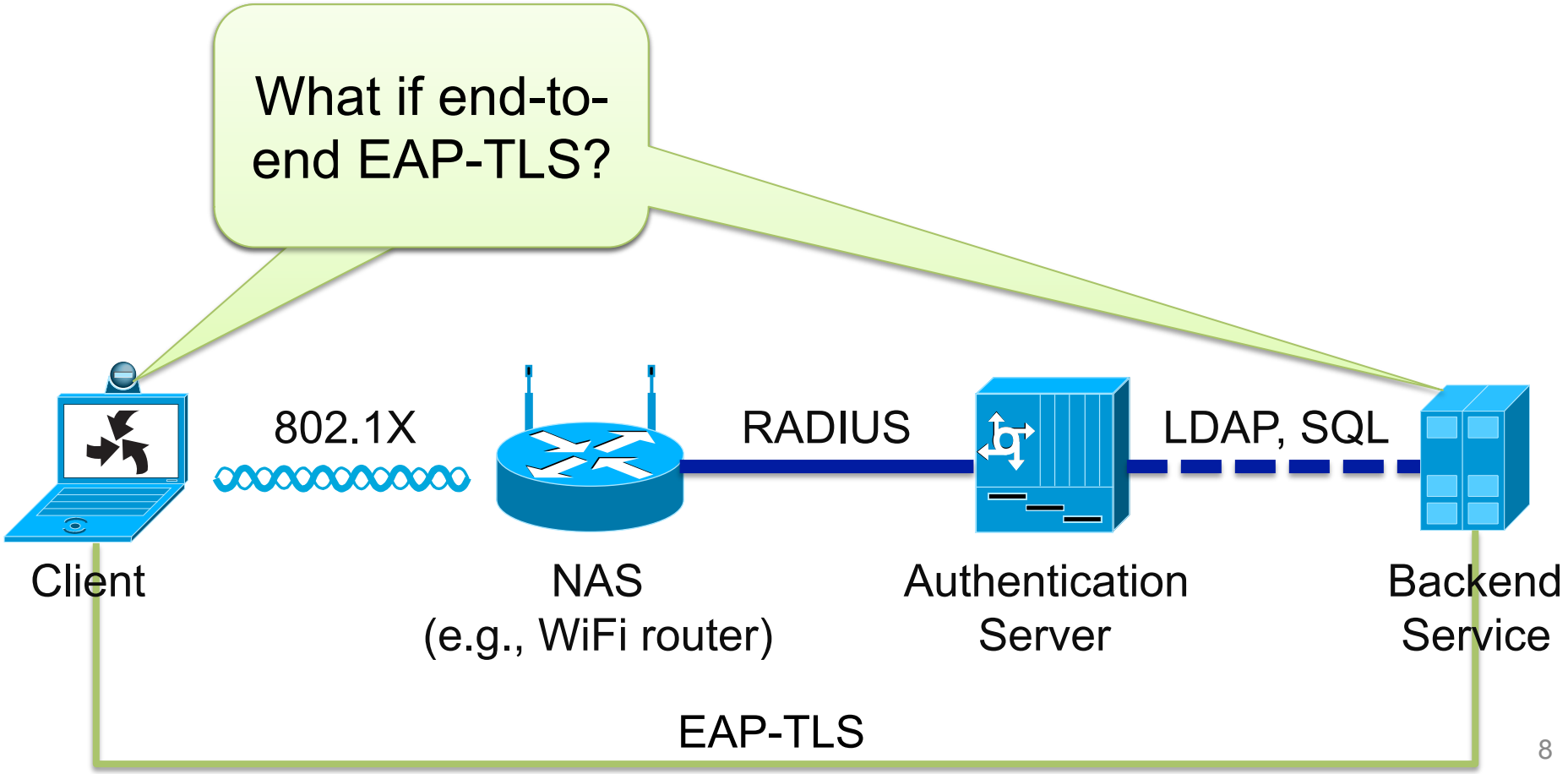
Authentication & Authorization Infra (AAI)

A typical Authentication & Authorization architecture in an enterprise network



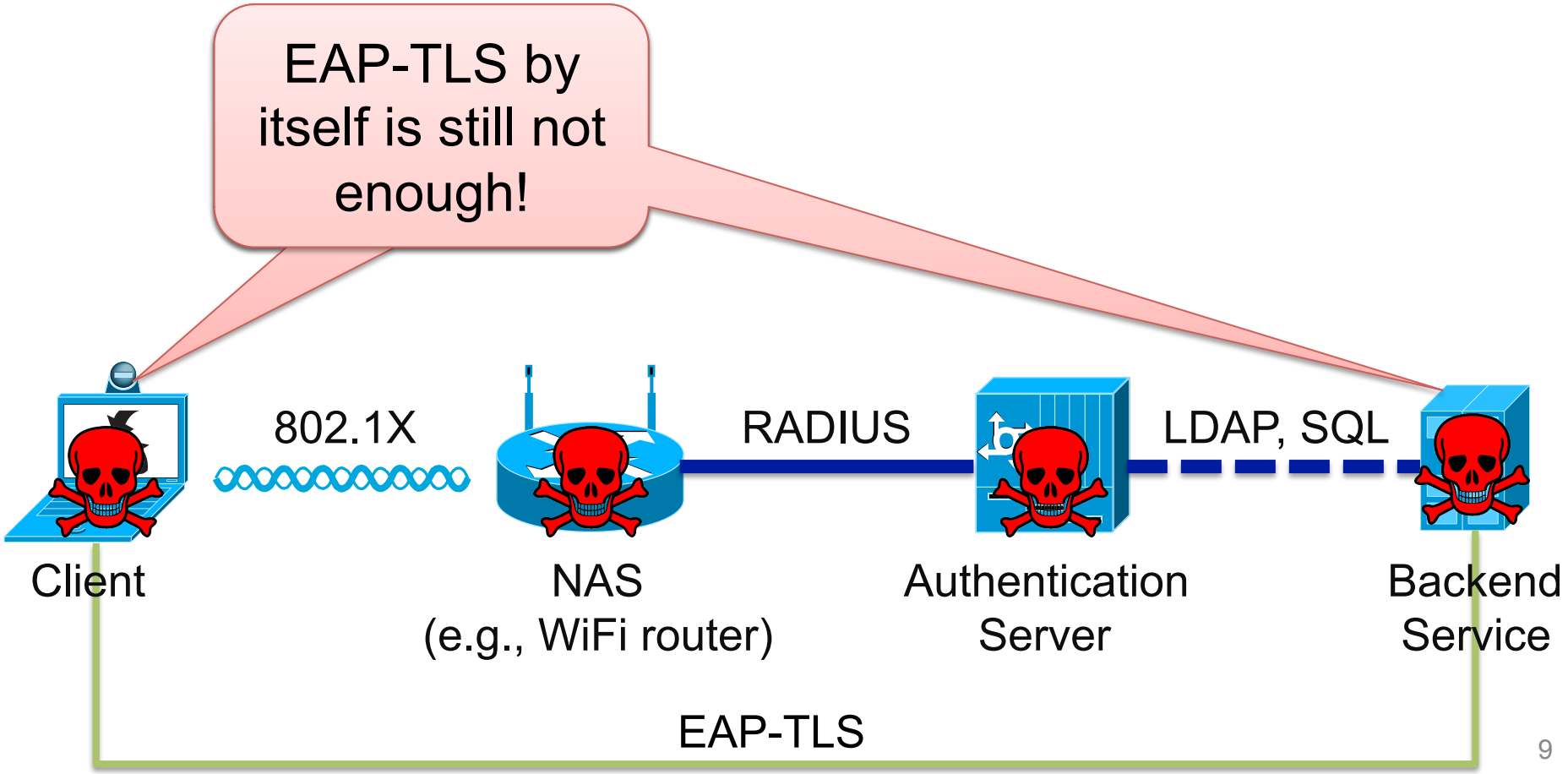
Authentication & Authorization Infra (AAI)

A typical Authentication & Authorization architecture in an enterprise network



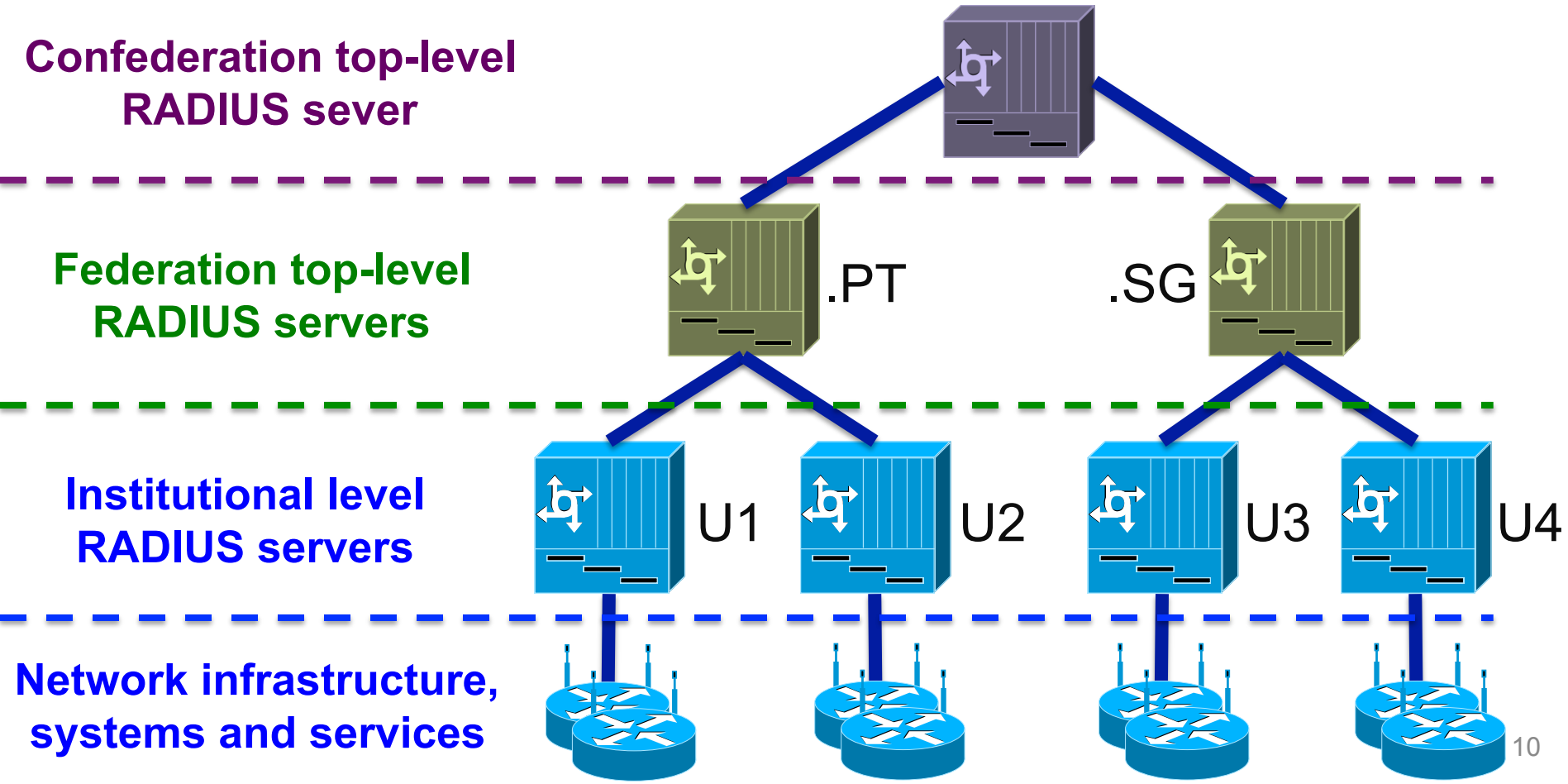
Authentication & Authorization Infra (AAI)

A typical Authentication & Authorization architecture in an enterprise network



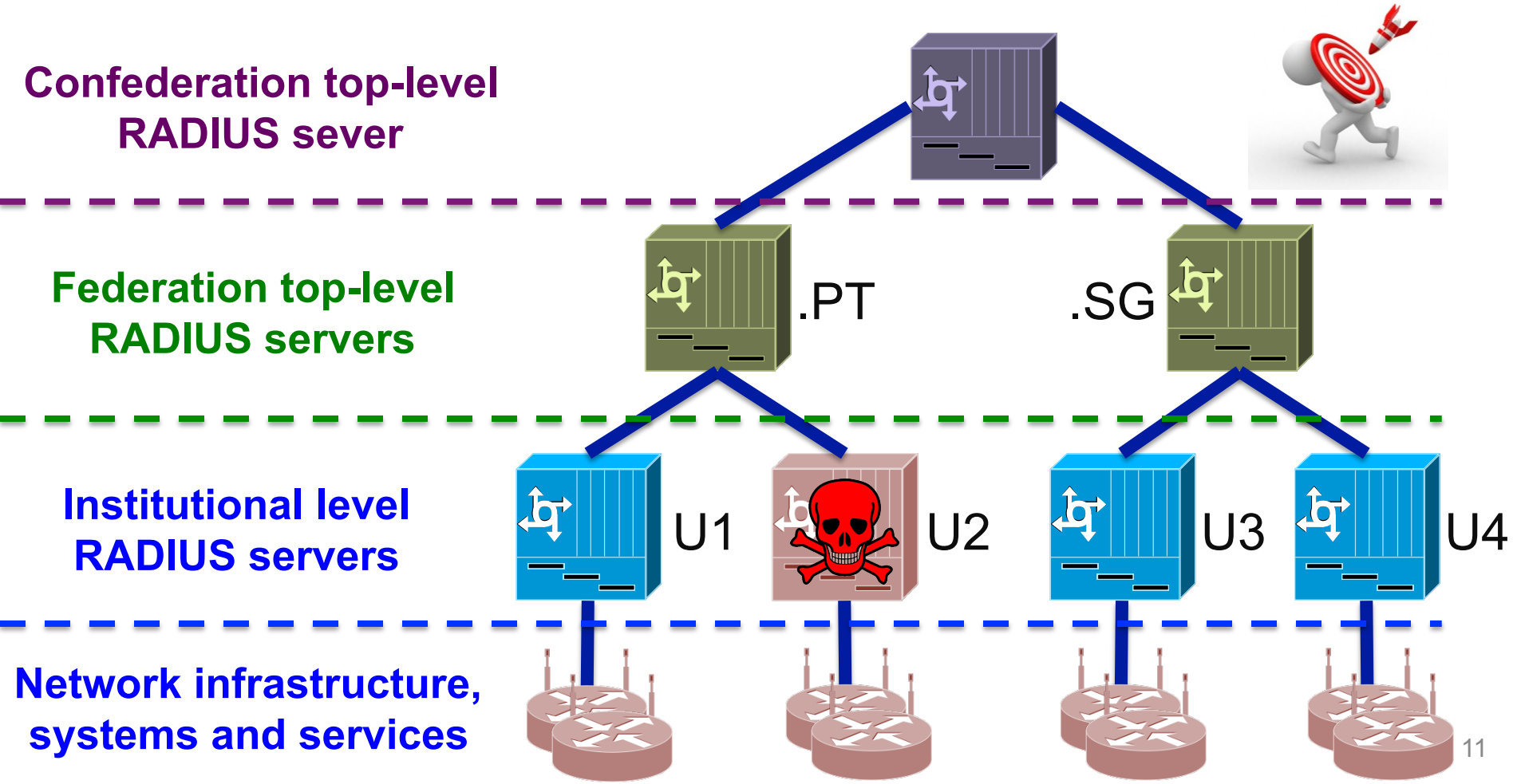
AAI Federations & Threats

A typical AAI **Federation**
among enterprise networks (mobility, …)



AAI Federations & Threats

A typical AAI **Federation**
among enterprise networks (mobility, …)



Outline

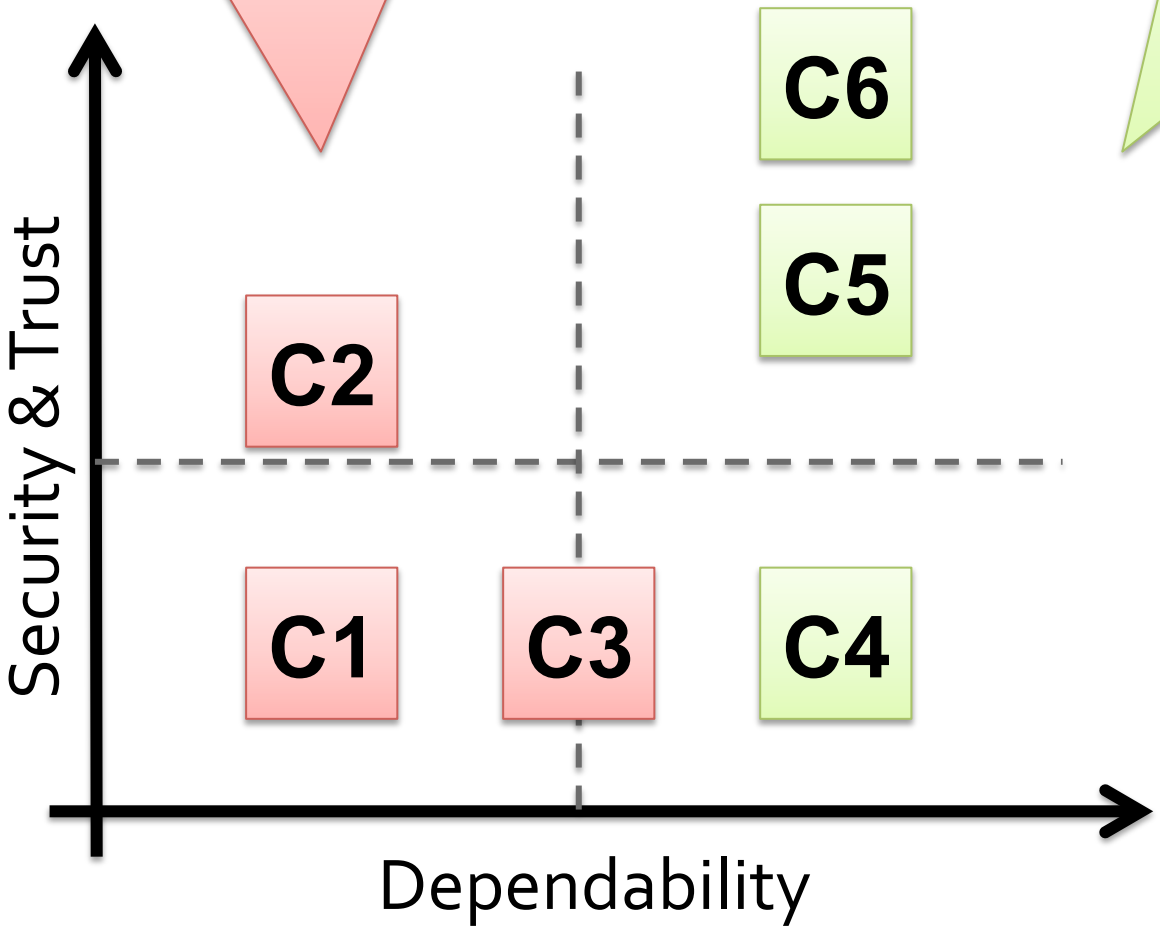
- **Goals & Challenges**
- Our Solution
- Intrusion-Tolerant AAIs
- Evaluation
- Conclusion

Mapping the current state of affairs of AAIs

Current State of Affairs of AAIs

Exiting systems are of categories C1, C2 and C43

Our goal is to design systems of categories C4-C6

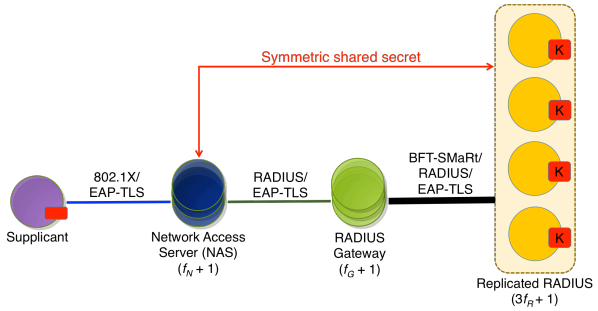


How to achieve our goals?

Approach 1: try to fix everything!?

How to achieve our goals?

Approach 2: increase the system's security and dependability



Hybrid system architectures, specialized components, clouds, …

Goals

Develop new **hybrid system architectures** for AAIs.

Design & Provide mechanisms for building **fault- and intrusion-tolerant** AAIs

Challenges

Arbitrary **fault tolerance** in AAI systems

Ensure **confidentiality of sensitive data**

Keep **backward compatibility**

Our main contributions

1. Step-by-step **design of resilient AAIs**
2. A **novel trusted component** for ensuring confidentiality
3. Experimental **evaluation in different environments**

Outline

Goals & Challenges

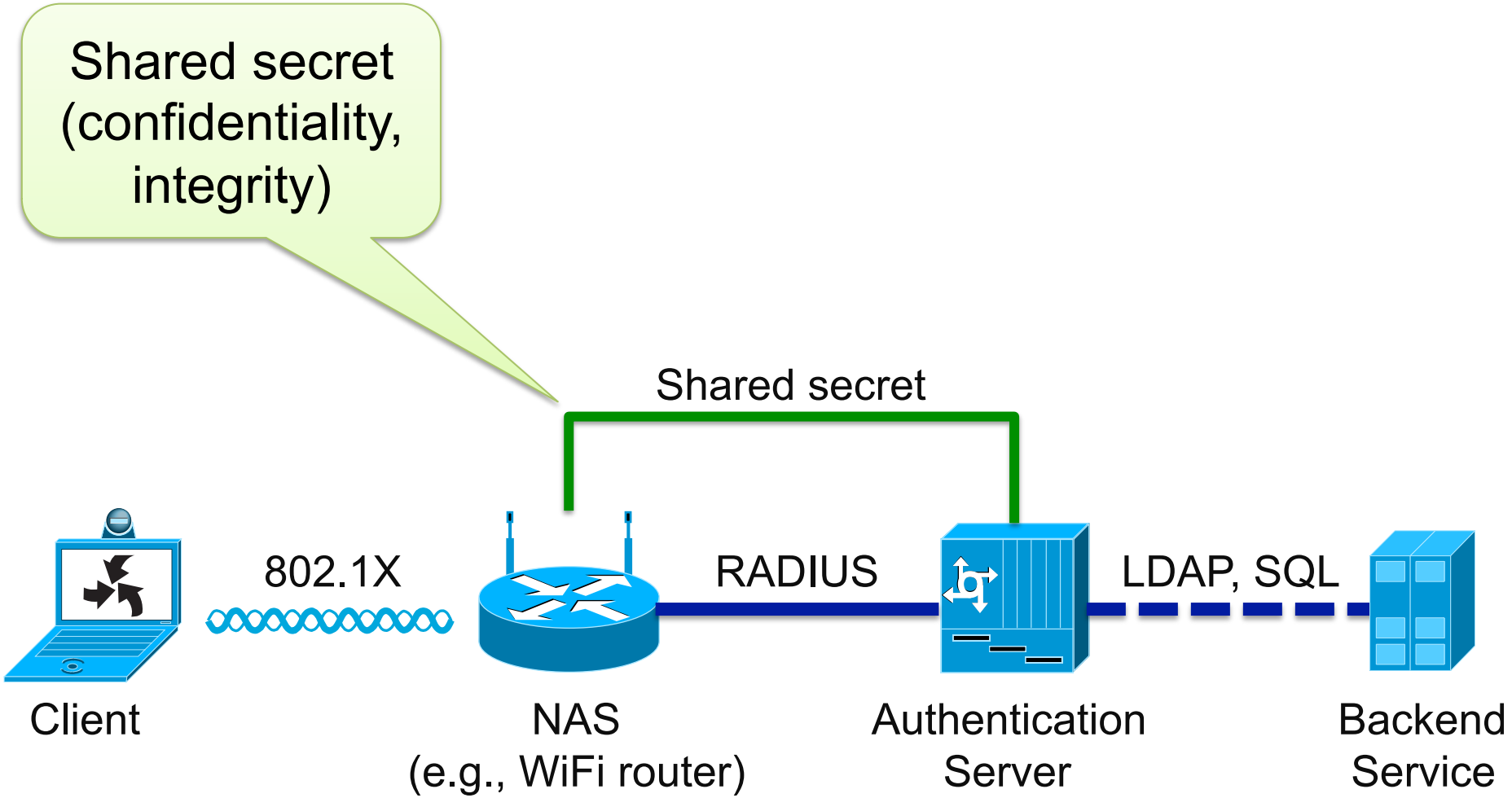
Our Solution

Intrusion-Tolerant AAIs

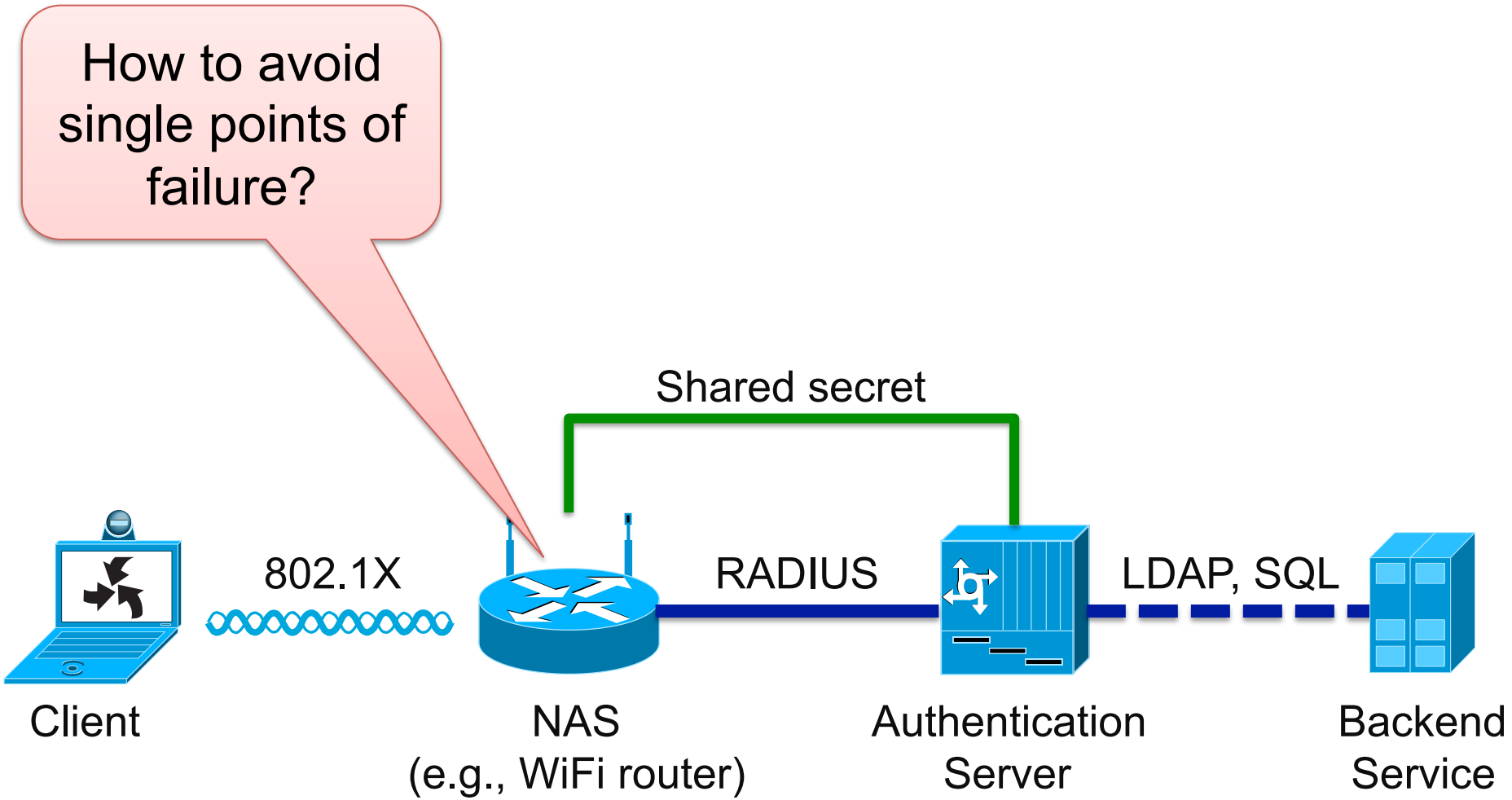
Evaluation

Conclusion

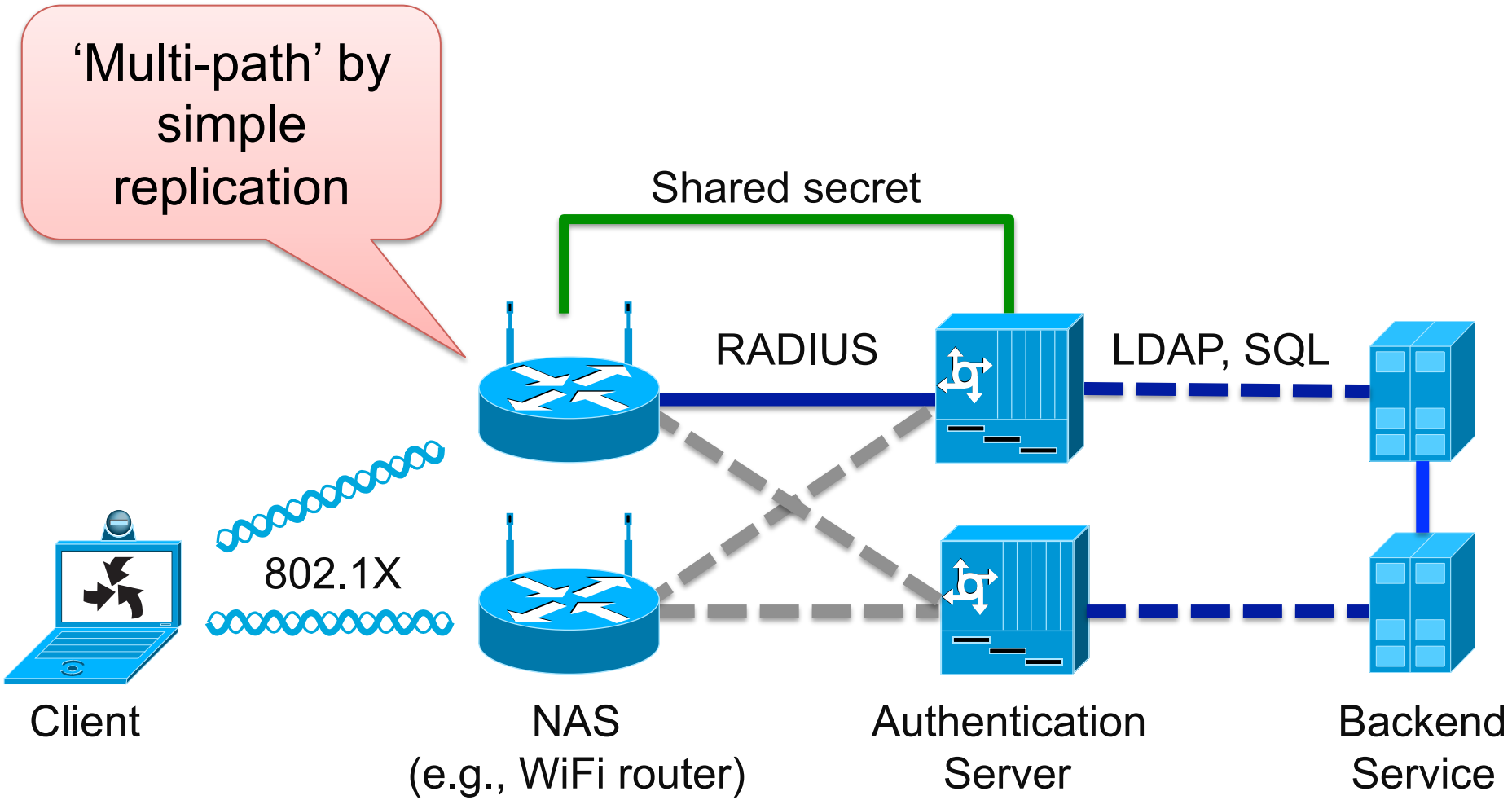
Traditional RADIUS architecture



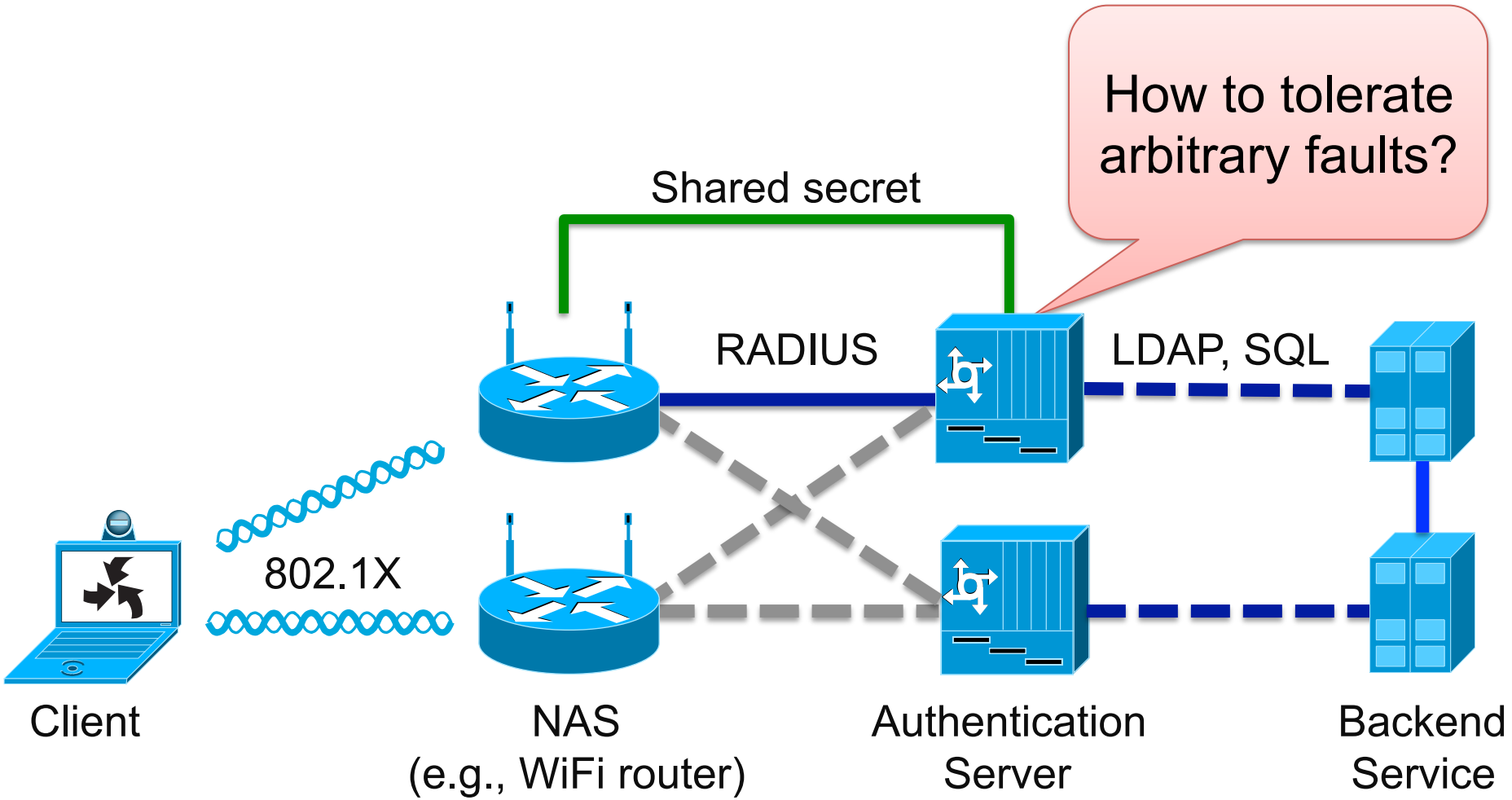
Traditional RADIUS architecture



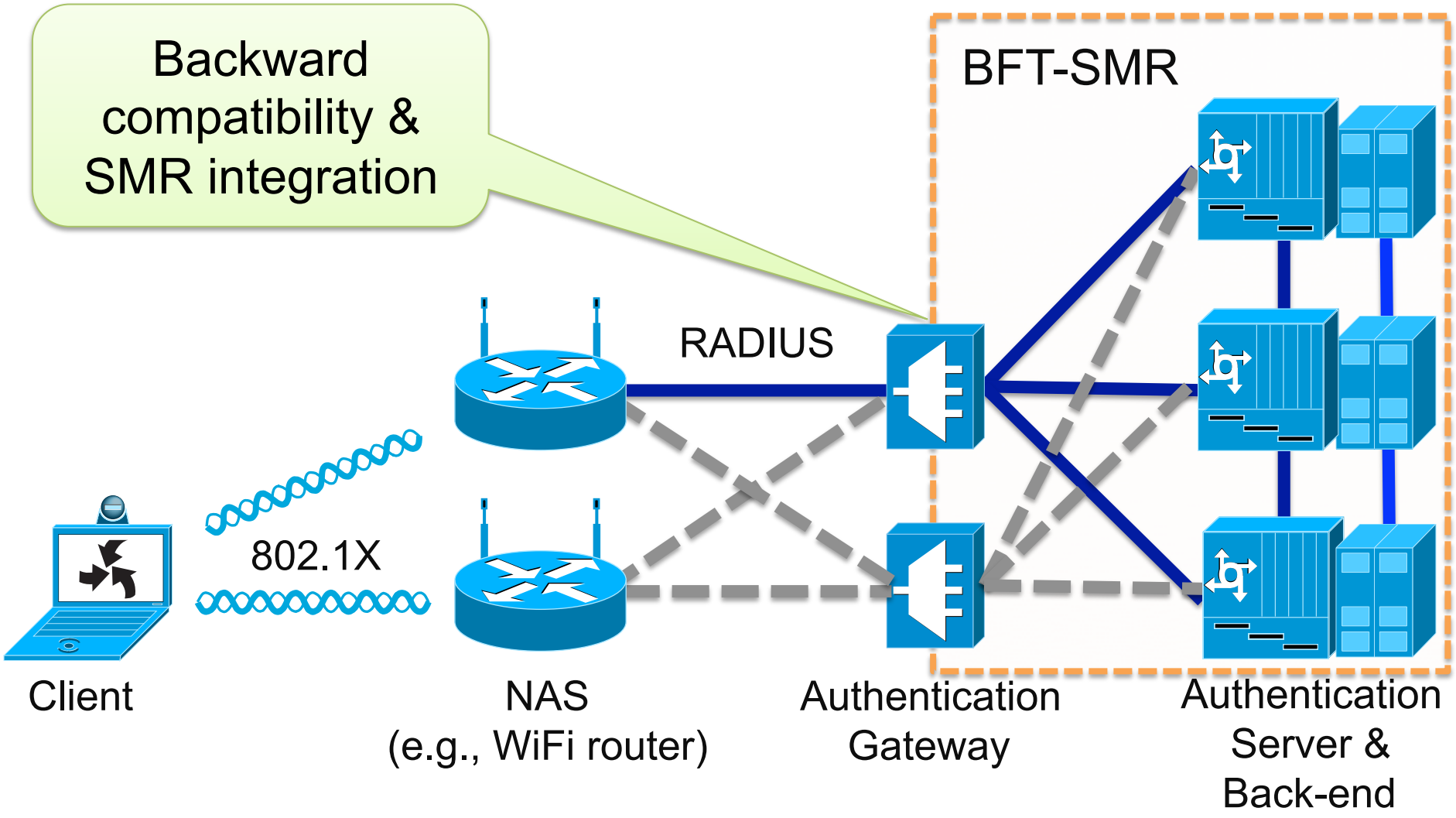
Building a resilient architecture



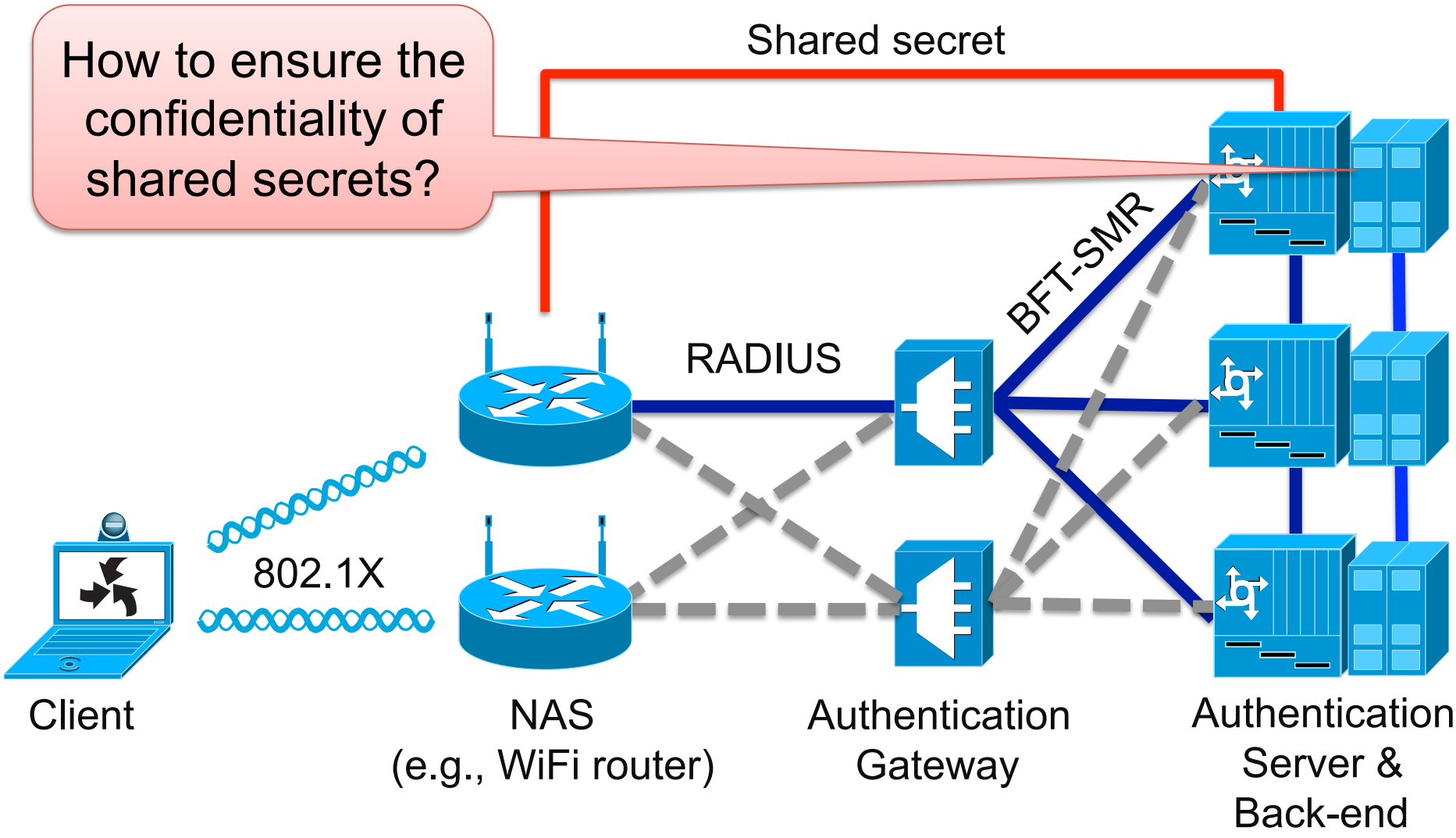
Building a resilient architecture



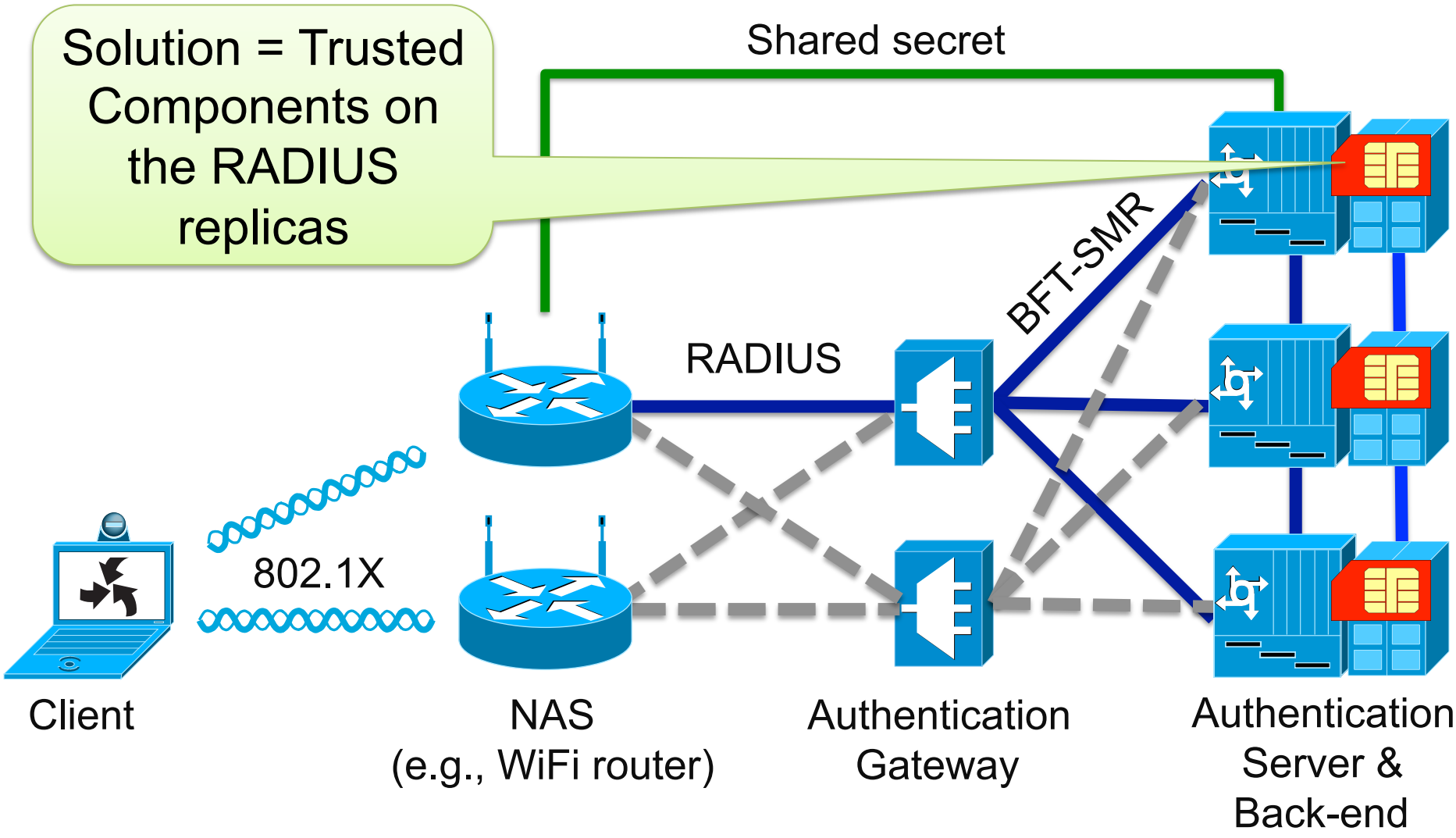
Building a resilient architecture



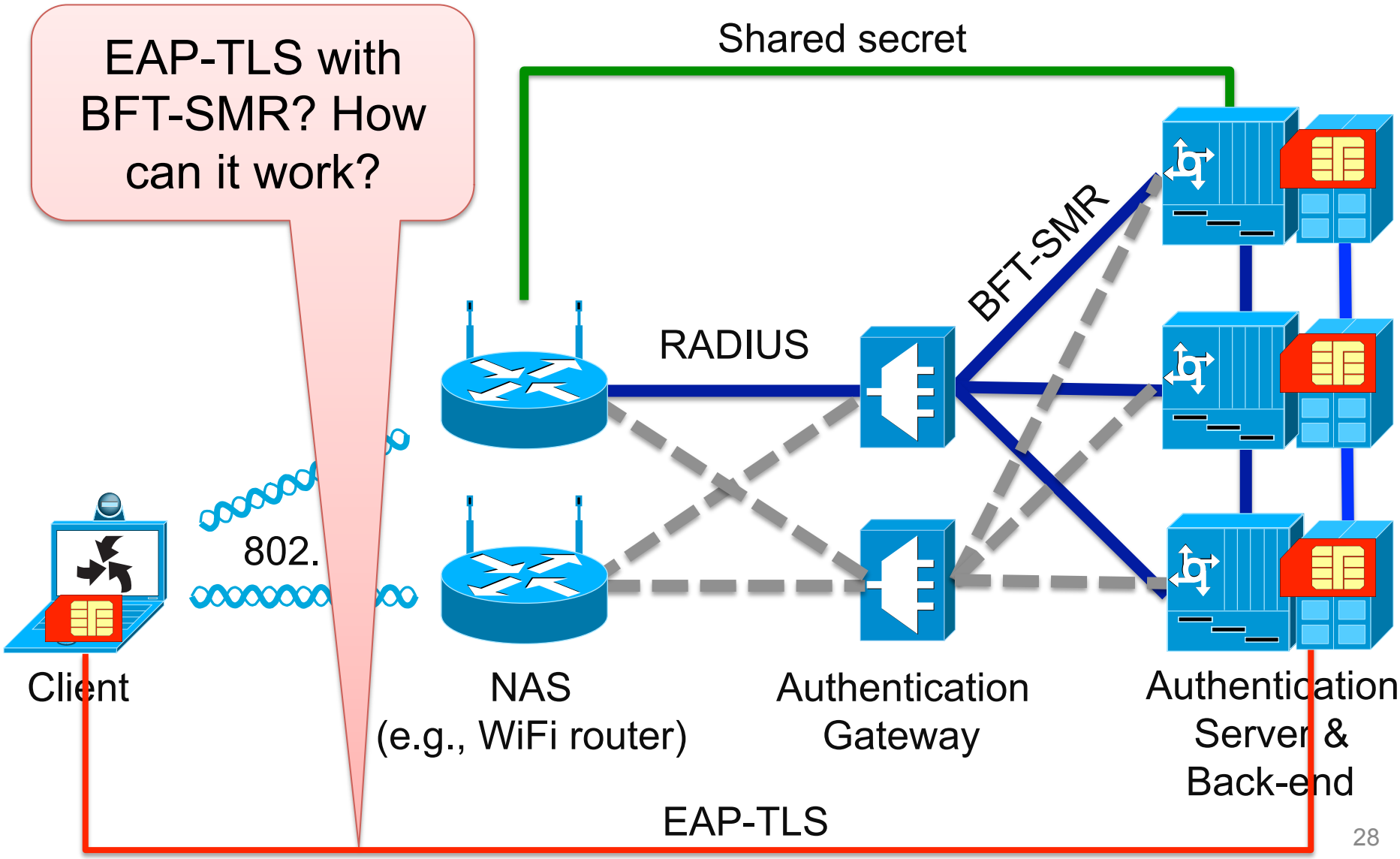
Building a resilient architecture



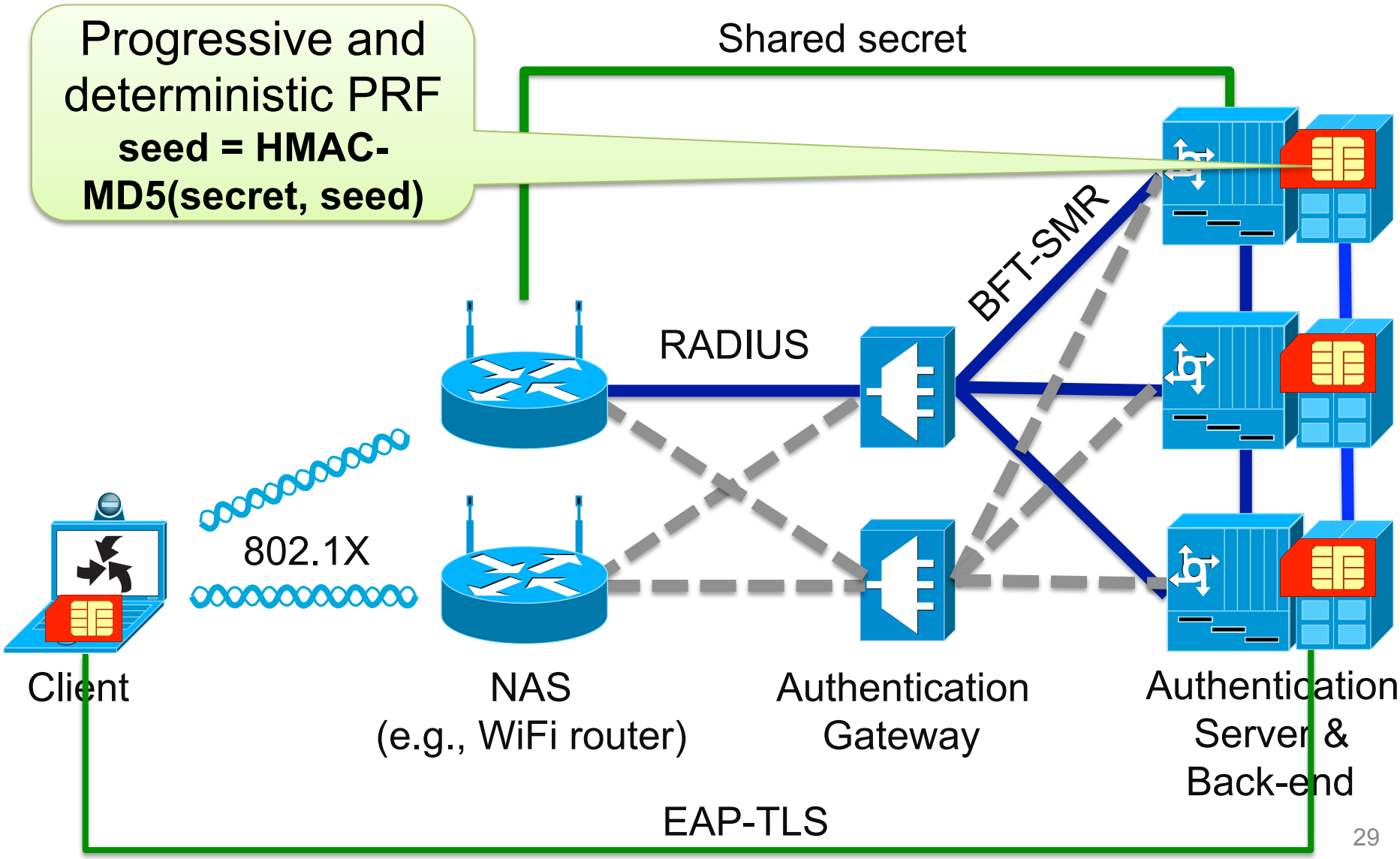
Building a resilient architecture



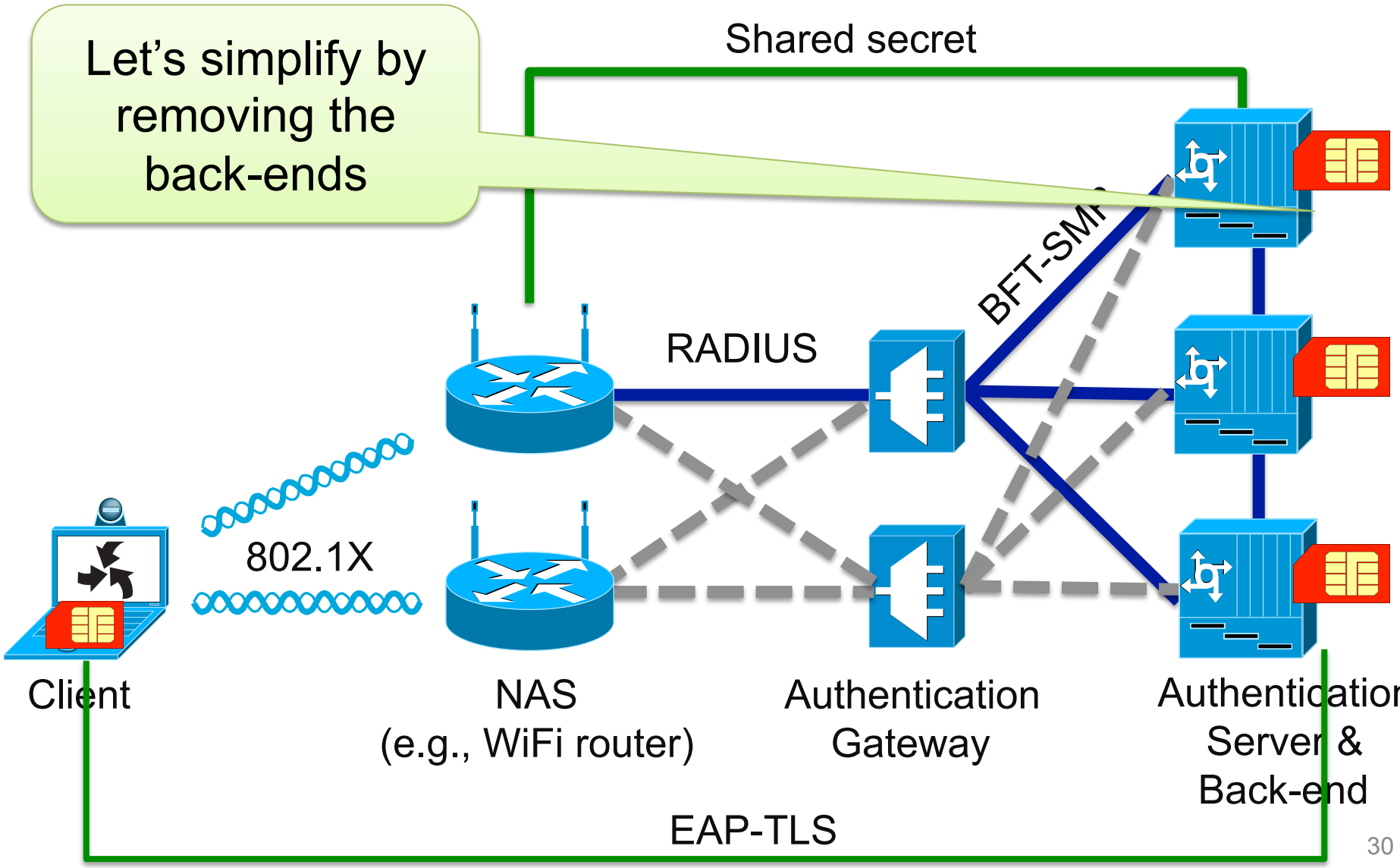
Building a resilient architecture



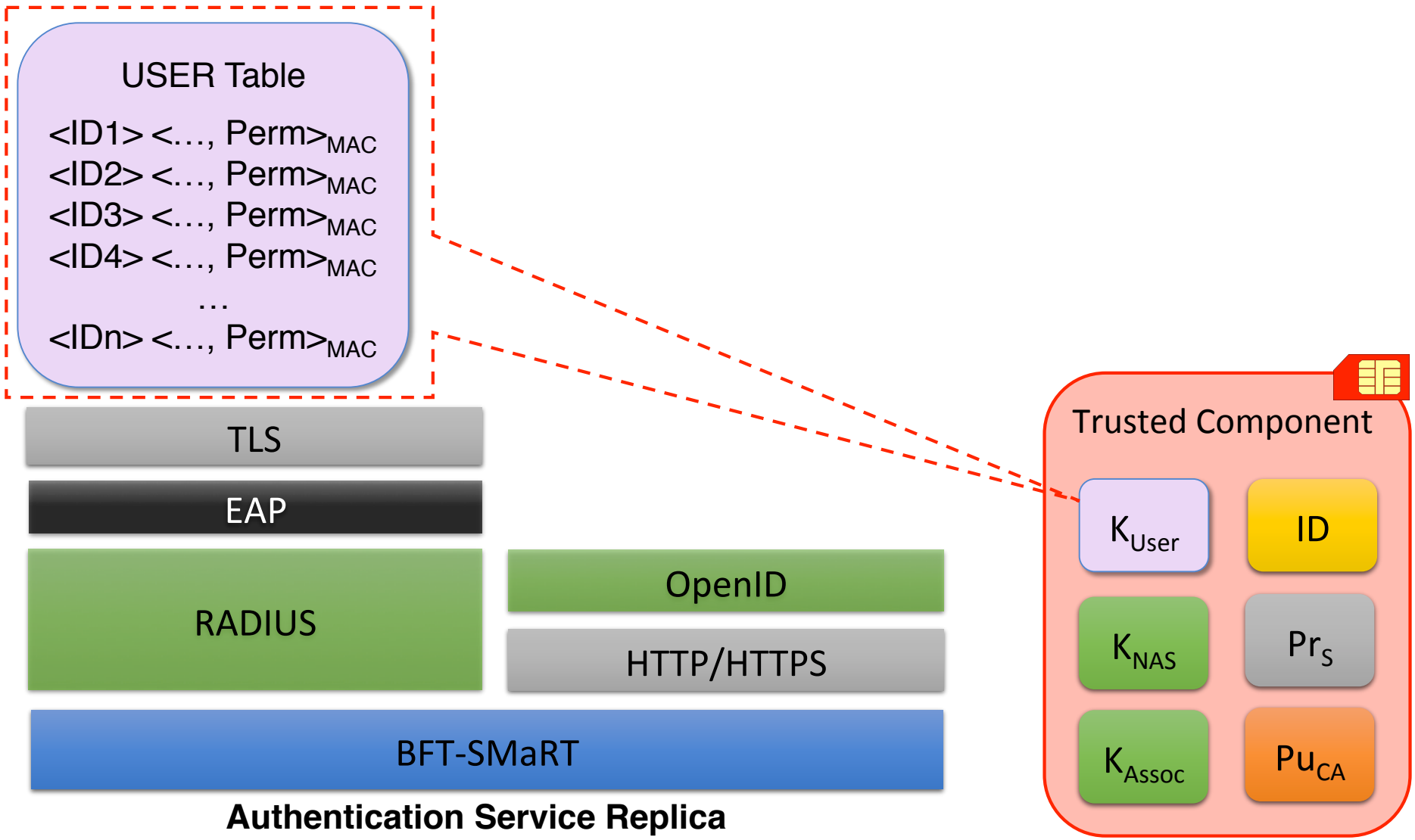
Building a resilient architecture



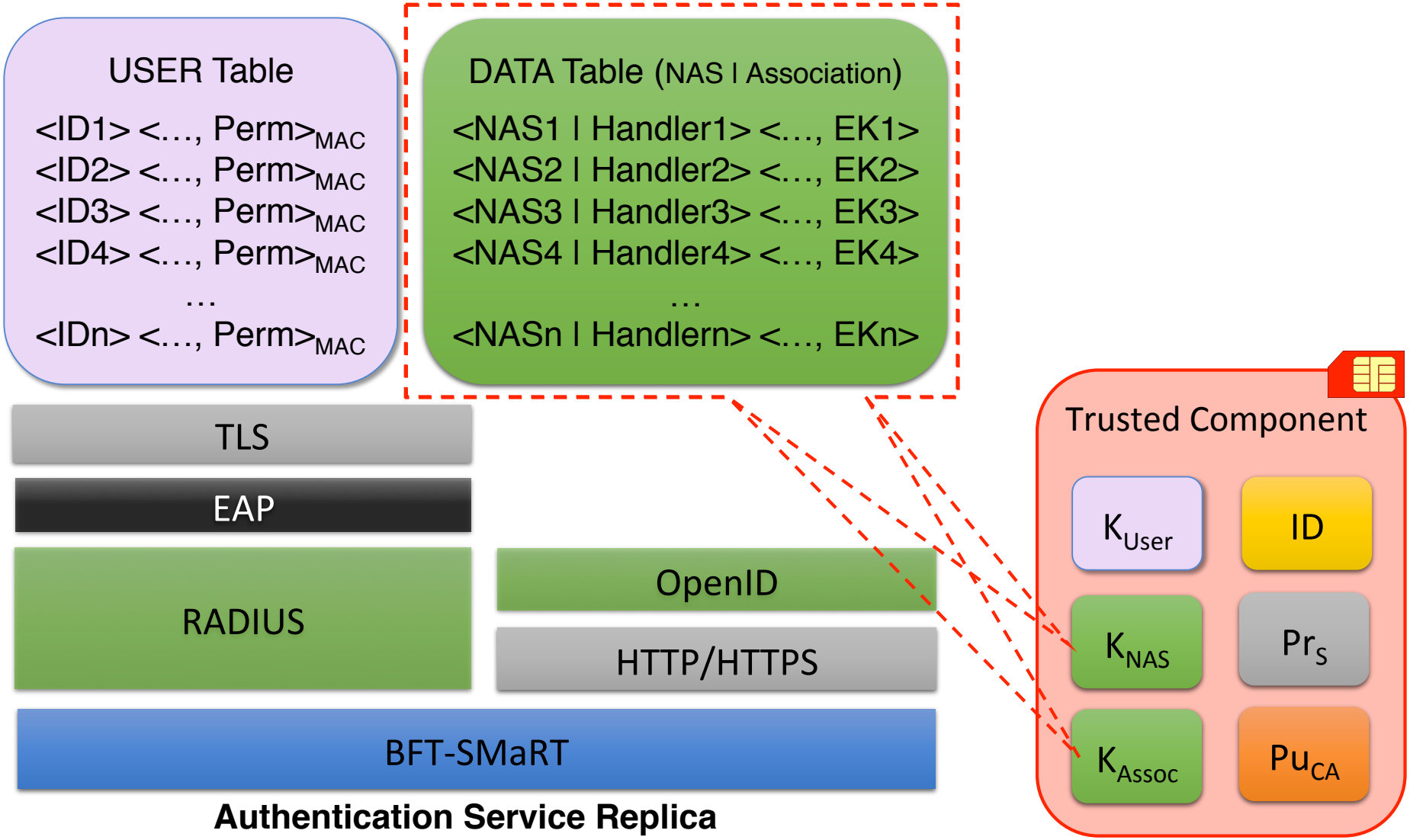
Building a resilient architecture



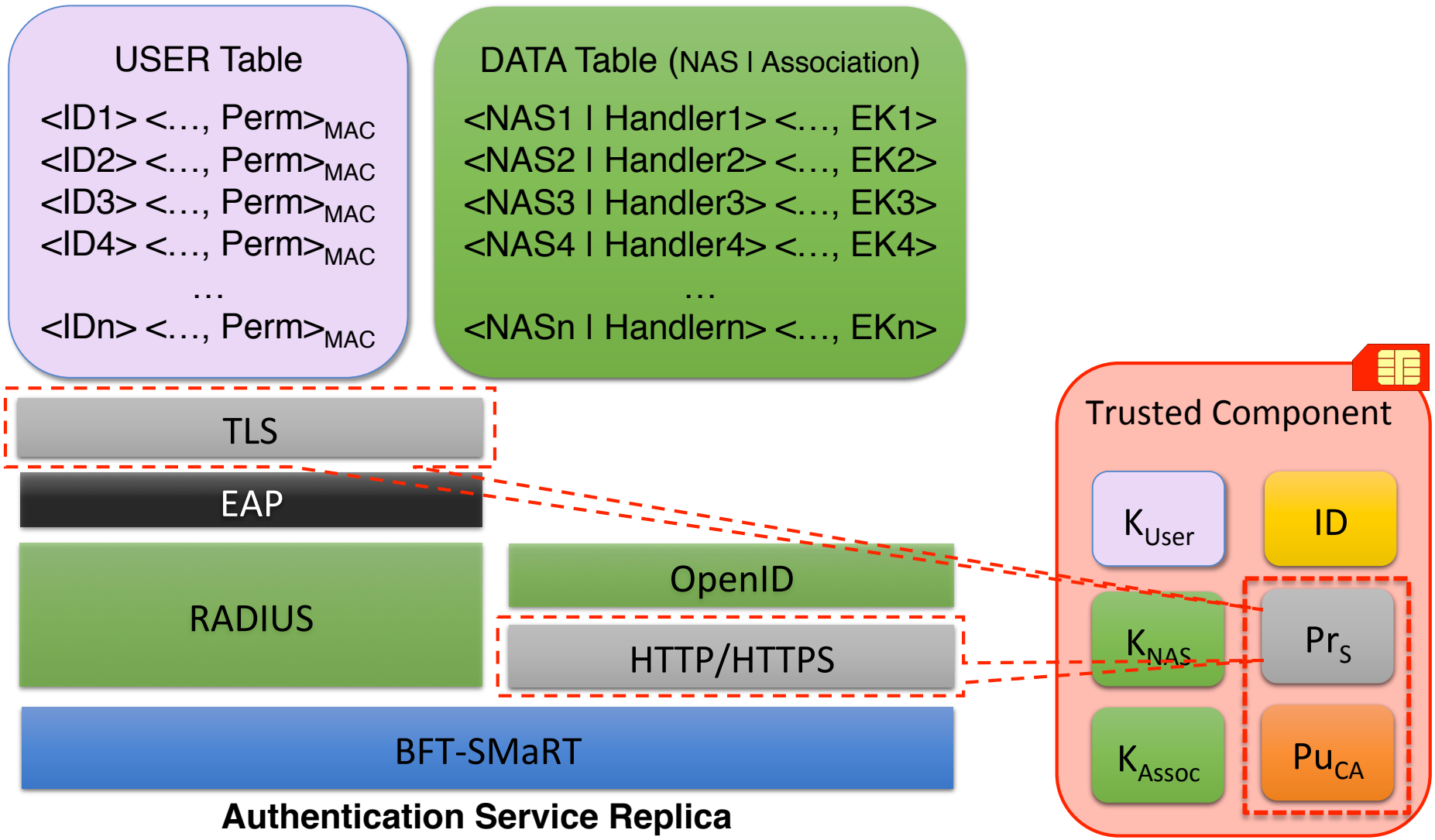
Sensitive Data & Trusted Component



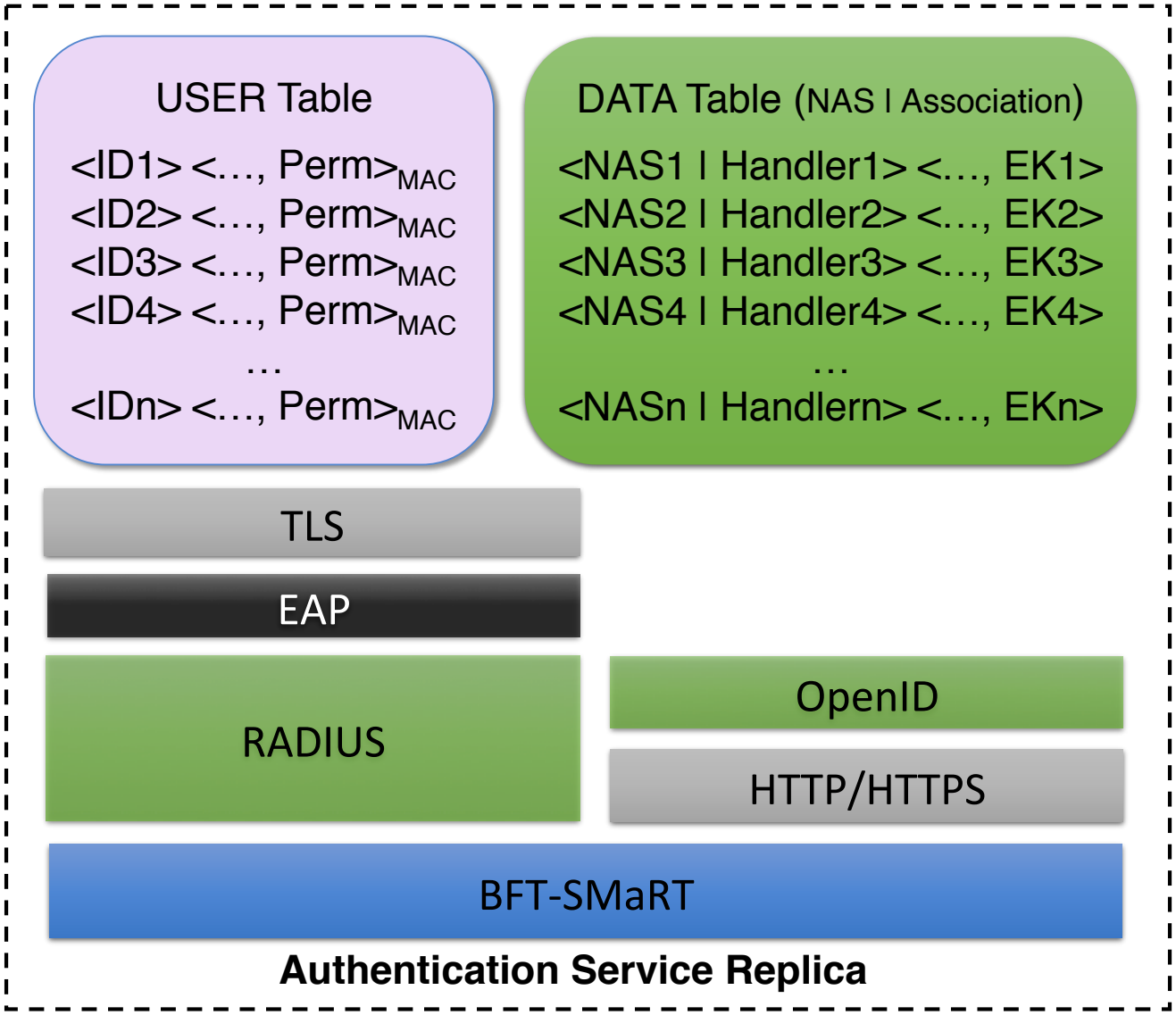
Sensitive Data & Trusted Component



Sensitive Data & Trusted Component

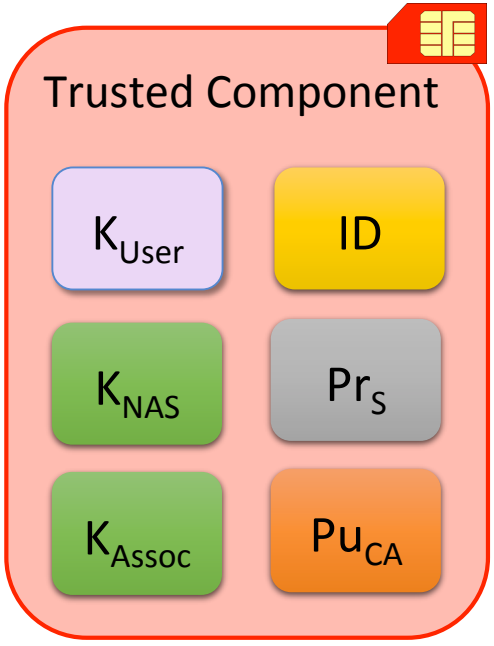


Sensitive Data & Trusted Component



SC methods:

1. HMAC
2. DecryptRSA
3. SymmCipher
4. Confidential
5. SignRSA
6. GenAssociation
7. GenNonce



Sensitive Data & Trusted Component

Method	Protocol	Input	Output
DecryptRSA	TLS	Packet to be verified.	Status of the signature verification.
SignRSA	TLS	Data to sign.	RSA signature using the key PrS .
SymmCipher	TLS/RADIUS	Protocol id and data.	Ciphered output of the input data.
Confidential	TLS/RADIUS	The packet data.	A confidential share of the data.
HMAC	RADIUS	data + encrypted shared key.	HMACMD5 of the input data.
GenAssoc	OpenID	Public key and two big integers.	Association info + server's public key.
GenNonce	OpenID	Two big integers.	Pseudo random nonce.

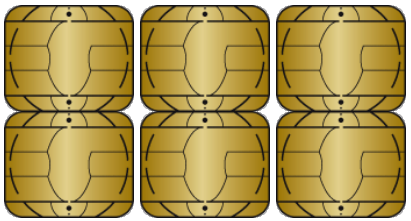
Sensitive Data & Trusted Component

Method	Protocol	Input	Output
DecryptRSA	TLS	Packet to be verified.	Status of the signature verification.
SignRSA	TLS	Data to sign.	RSA signature using the key PrS .
SymmCipher	TLS/RADIUS	Protocol id and data.	Ciphered output of the input data.
Confidential	TLS/RADIUS	The packet data.	A confidential share of the data.
HMAC	RADIUS	data + encrypted shared key.	HMACMD5 of the input data.
GenAssoc	OpenID	Public key and two big integers.	Association info + server's public key.
GenNonce	OpenID	Two big integers.	Pseudo random nonce.

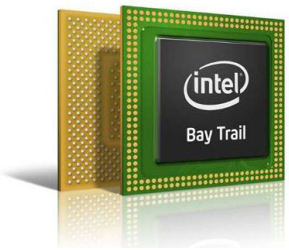
How to implement a trusted component?

*A trusted component can be **"any" device capable of ensuring the data and operation confidentiality** of the target system/environment.*

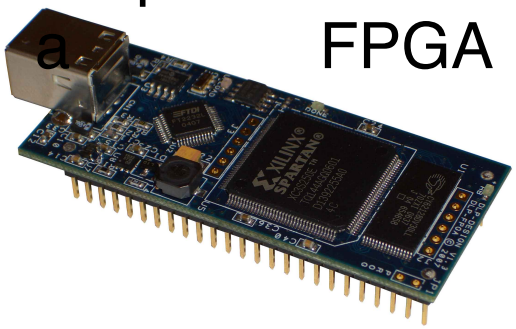
Smart Cards



Intel SGX

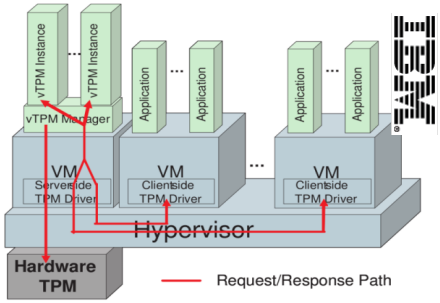


Tamper Resistant FPGA

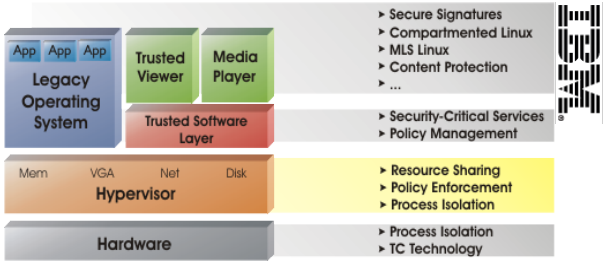


A Highly Secured (shielded) Computer

Virtual TPM (e.g. vTPM)

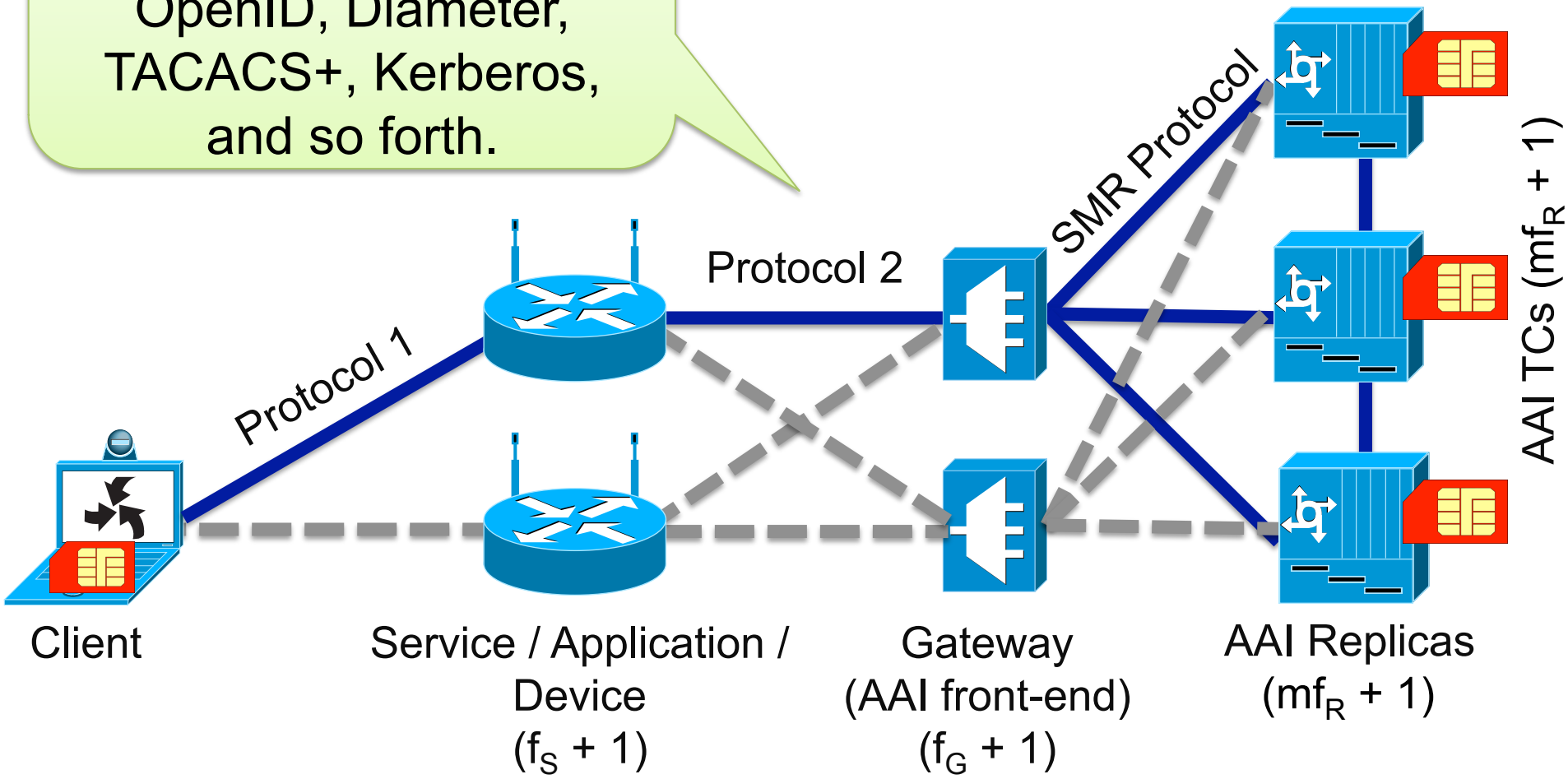


Secure Hypervisor (e.g. sHyper)

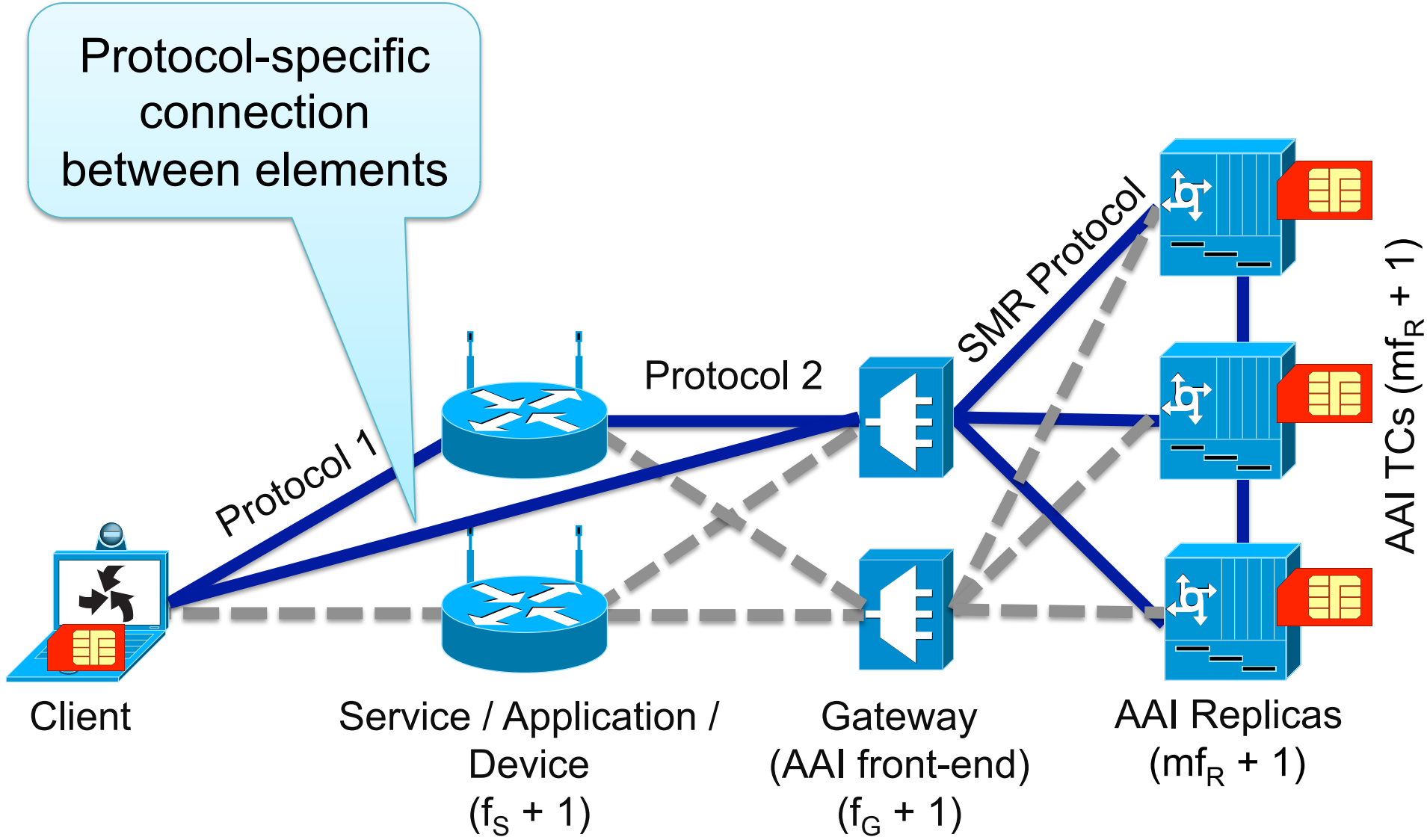


Generic resilient architecture for AAIs

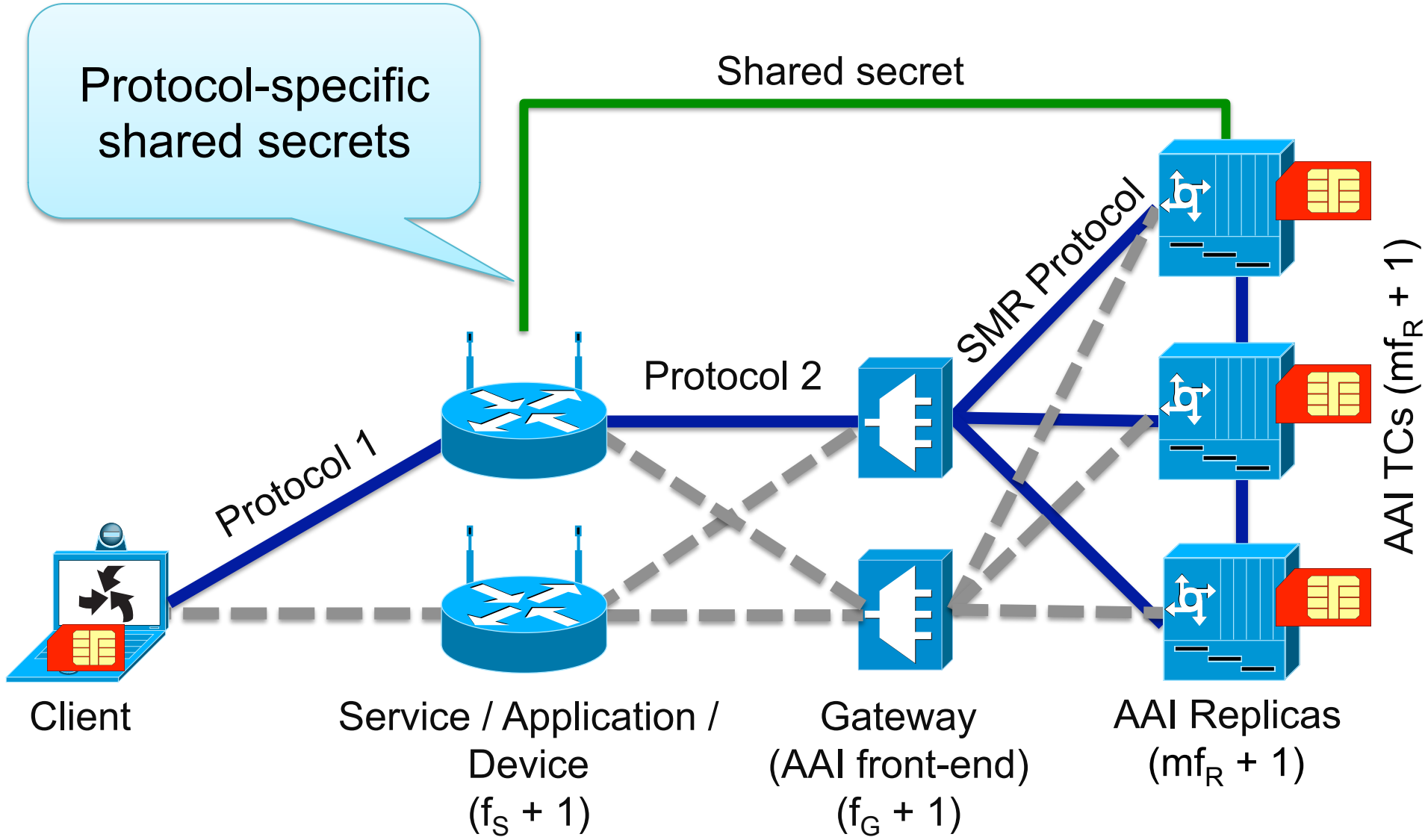
Suitable for services such as RADIUS, OpenID, Diameter, TACACS+, Kerberos, and so forth.



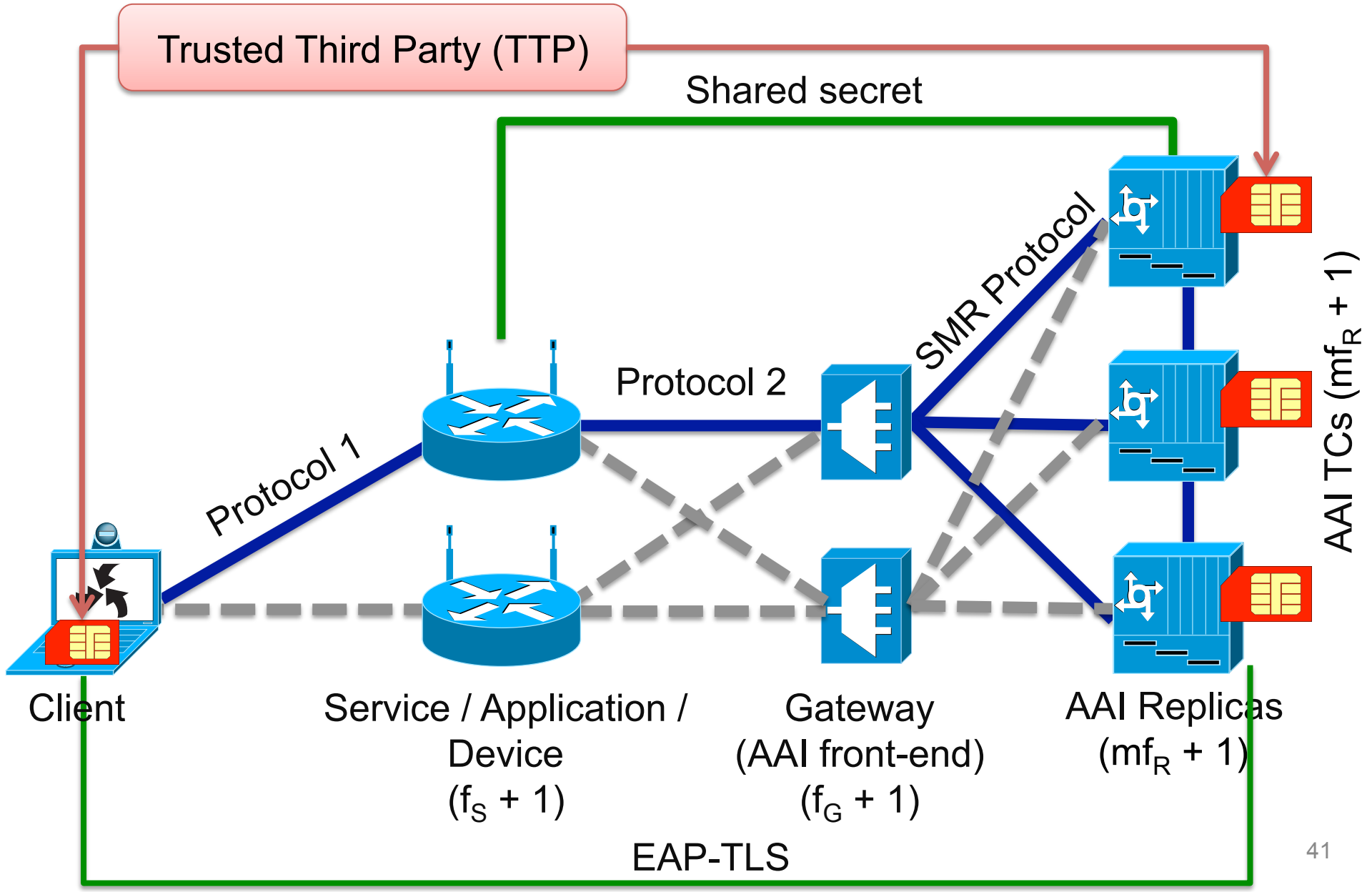
Generic resilient architecture for AAIs



Generic resilient architecture for AAIs



Generic resilient architecture for AAIs



Outline

Goals & Challenges

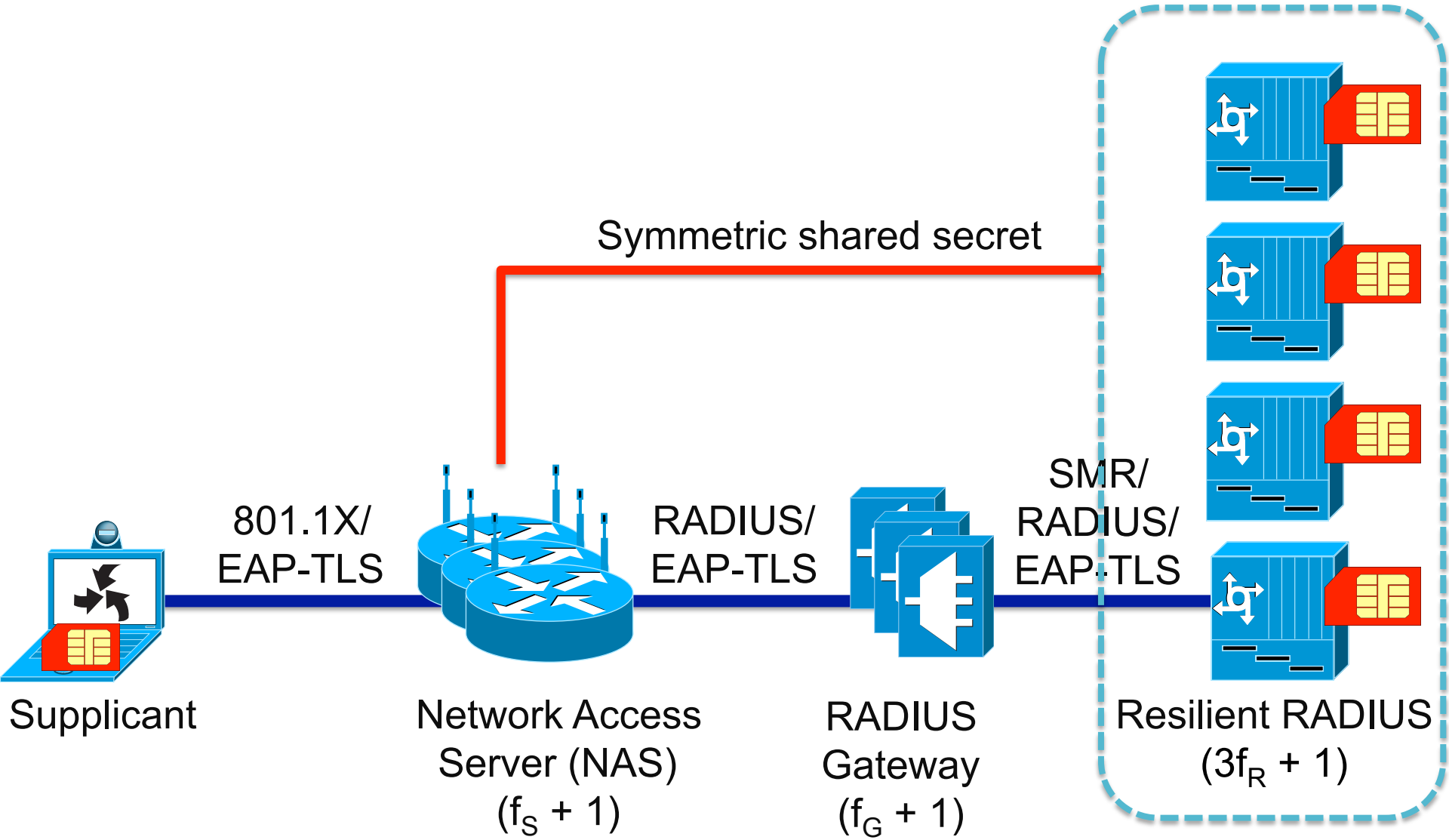
Our Solution

Intrusion-Tolerant AAIs

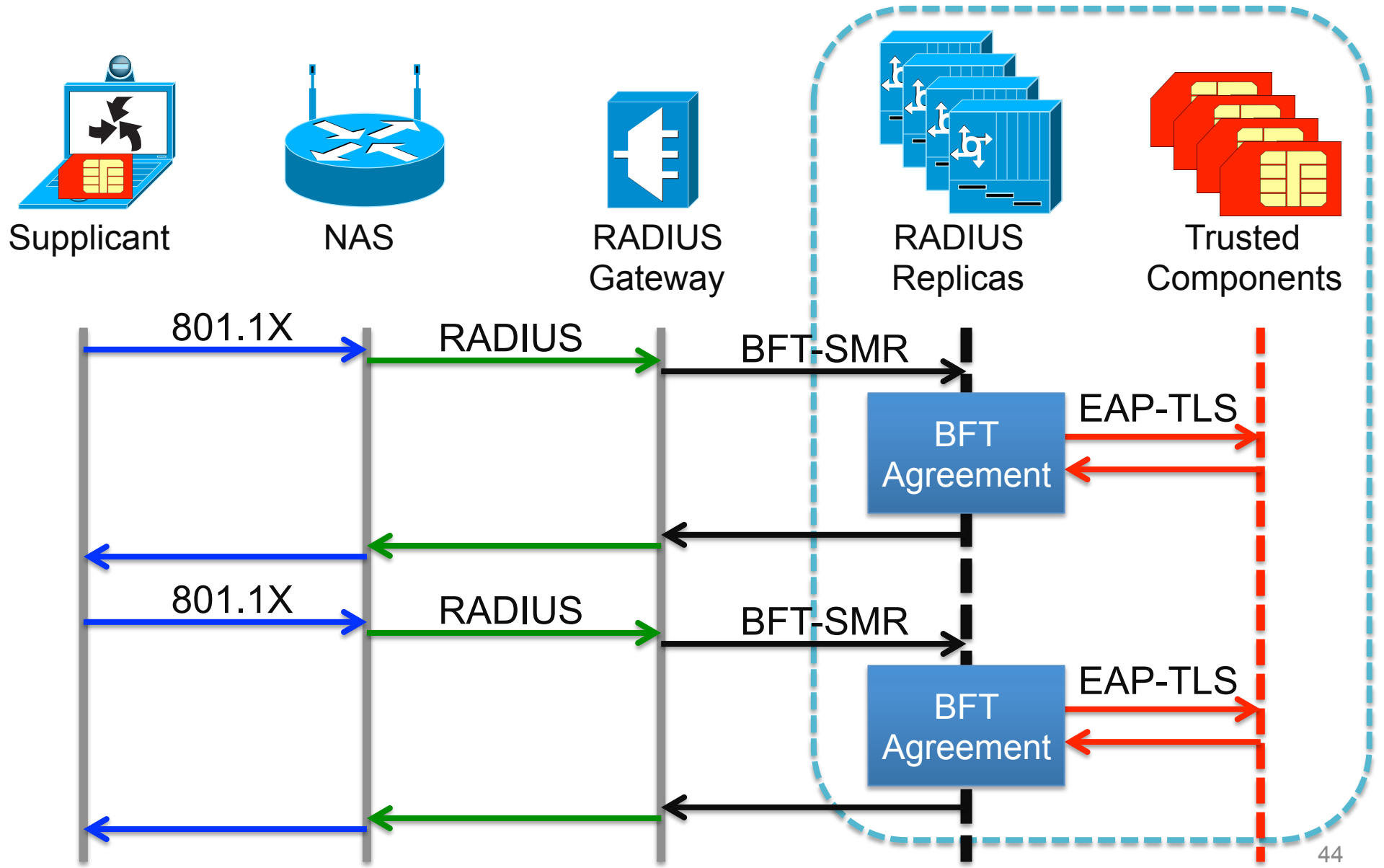
Evaluation

Conclusion

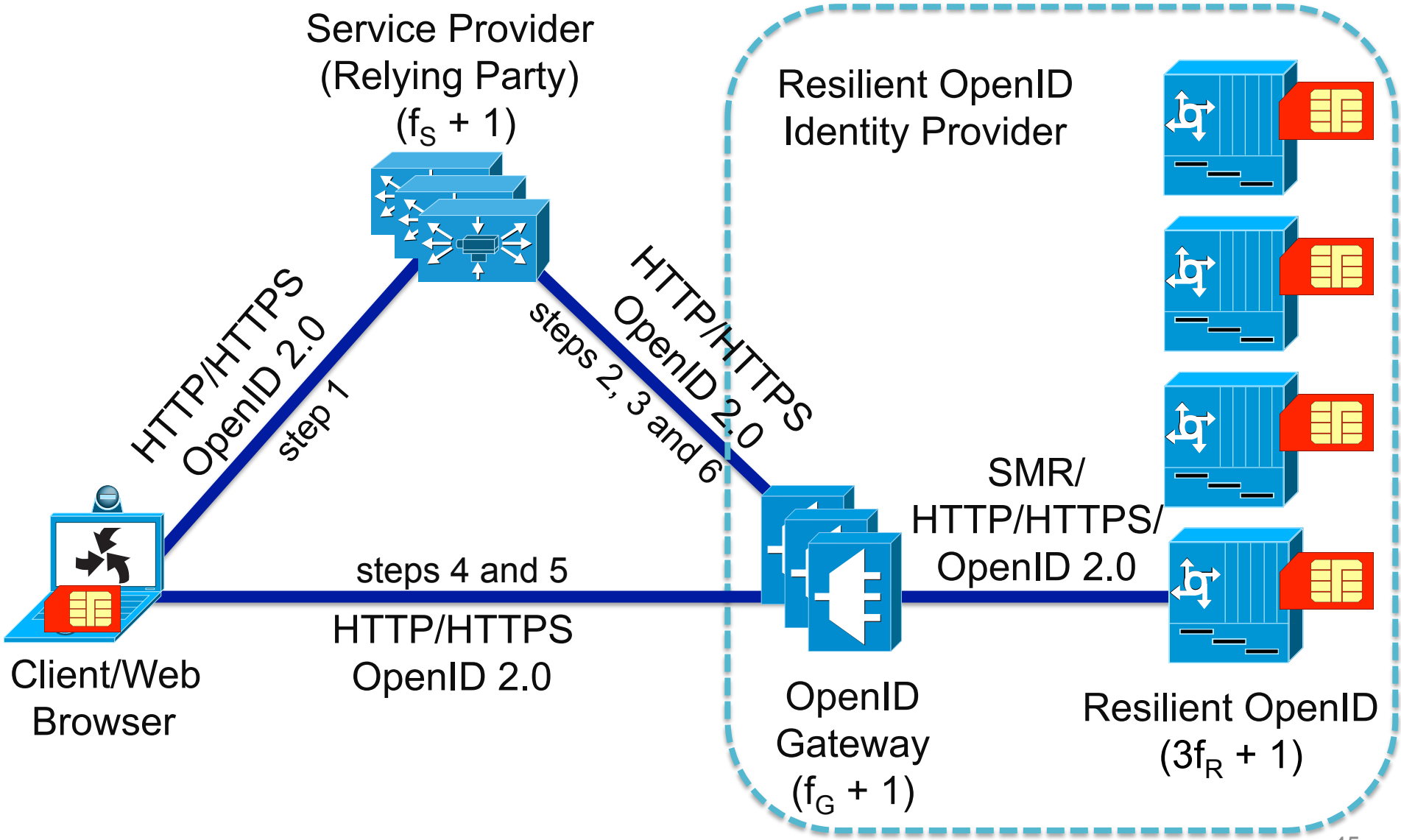
Resilient RADIUS architecture



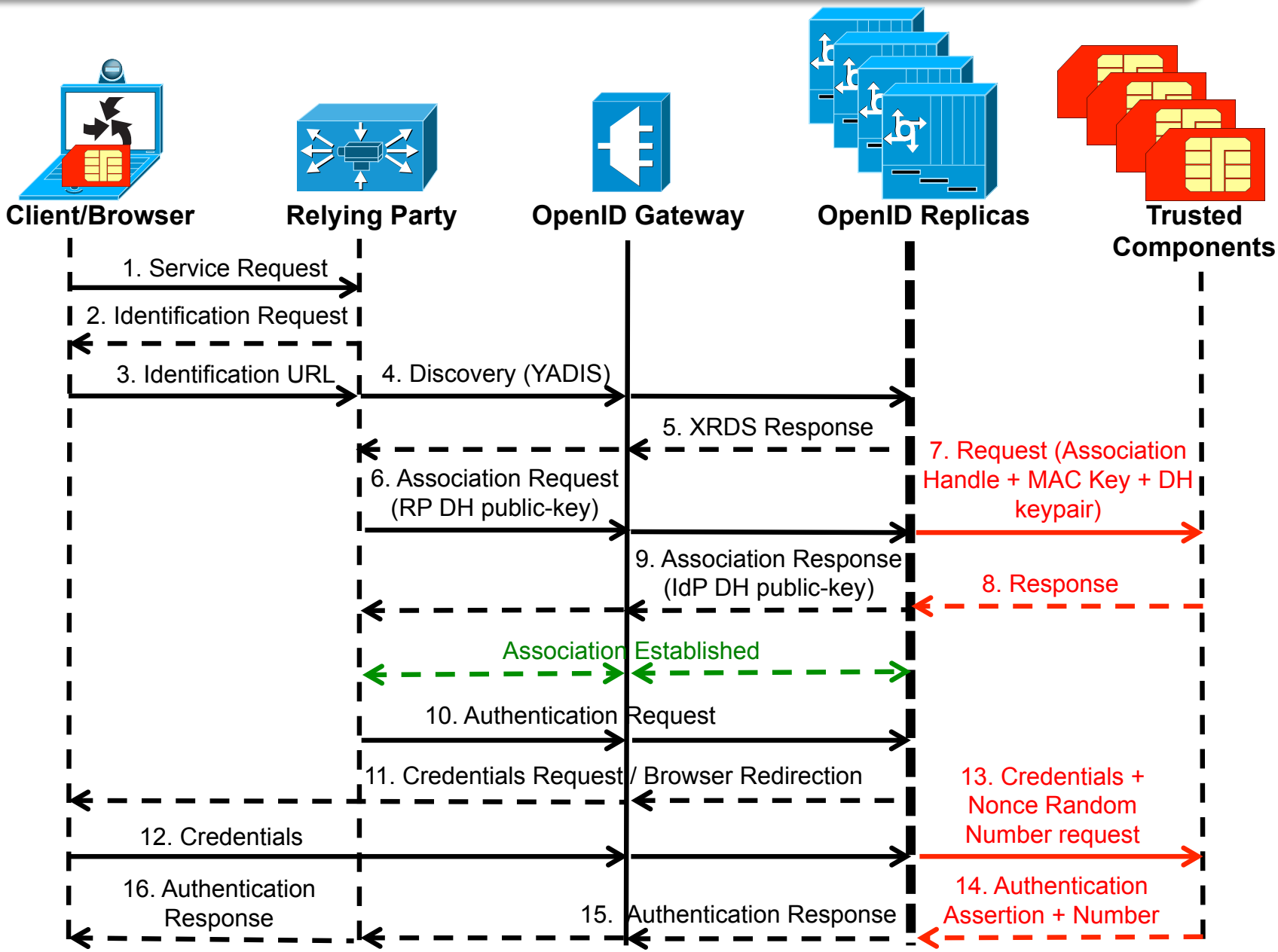
Resilient RADIUS communications



Resilient OpenID architecture



Resilient OpenID communications



Outline

Goals & Challenges

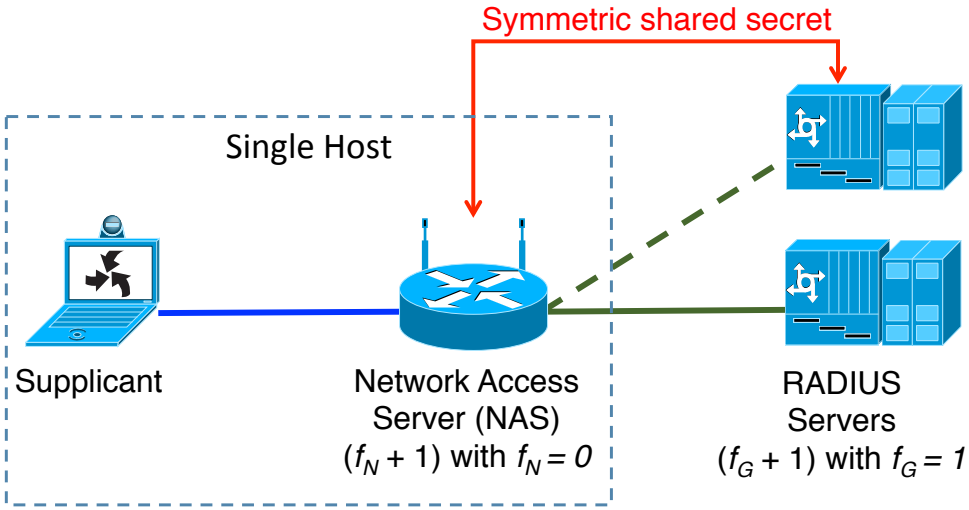
Our Solution

Intrusion-Tolerant AAIs

Evaluation

Conclusion

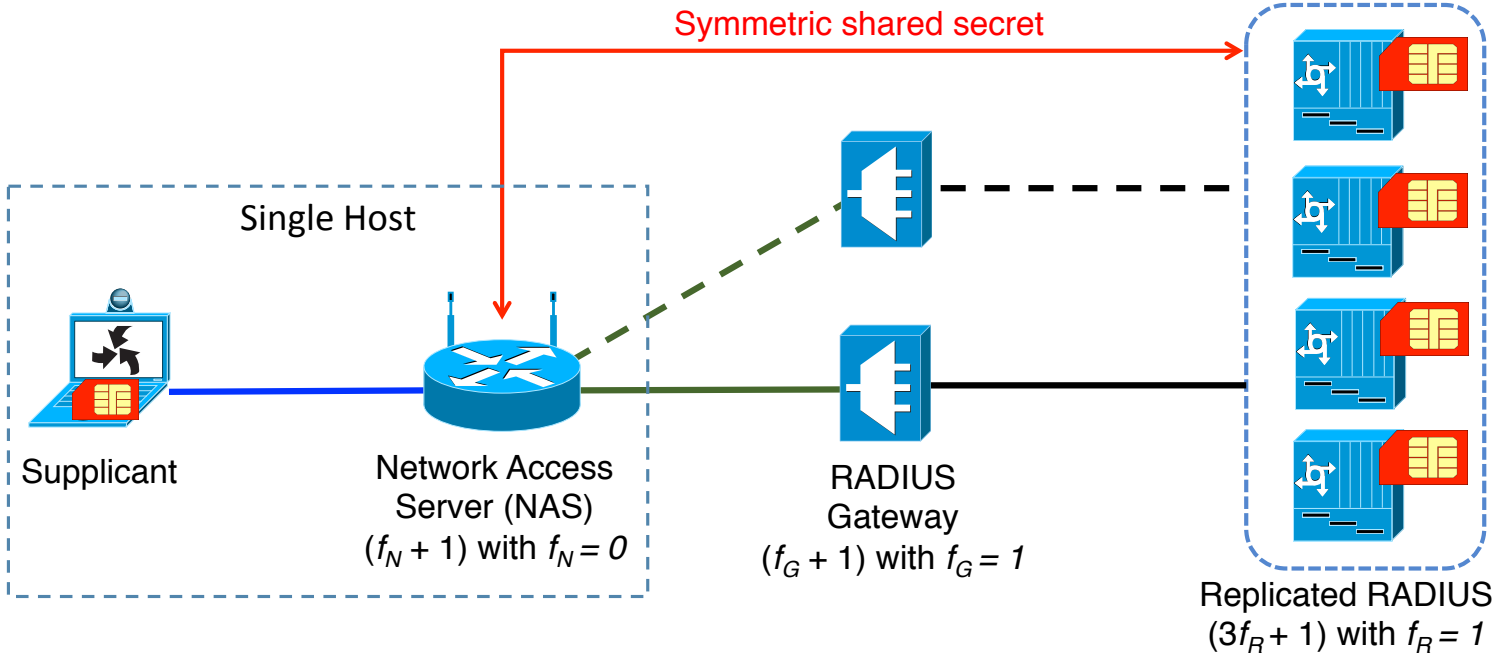
Resilient RADIUS vs FreeRADIUS



Environment / Configuration

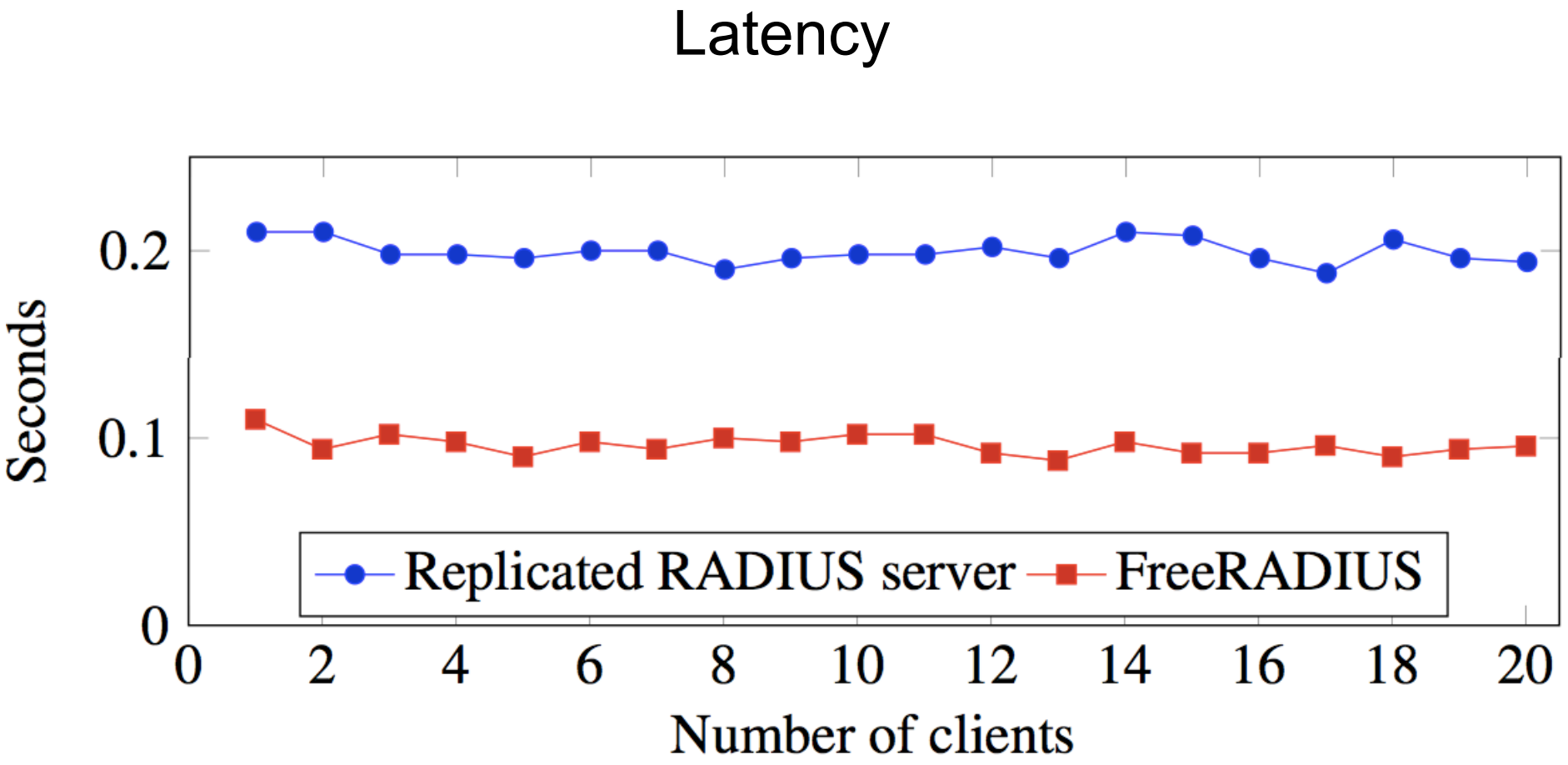
CPU	MEM	Net
2x4	32G	Giga

FreeRADIUS
3 machines

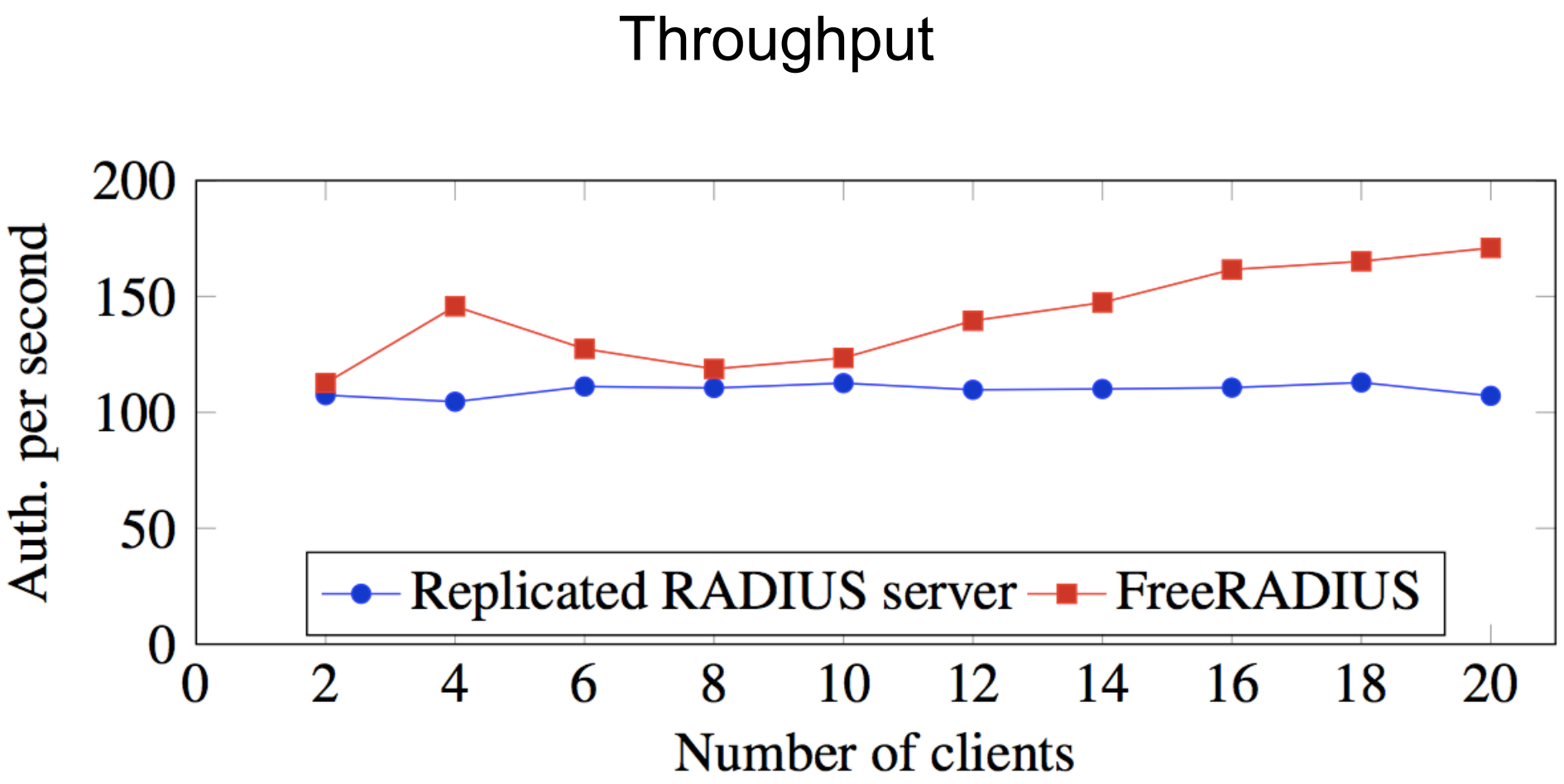


Resilient
RADIUS
7 machines

Resilient RADIUS vs FreeRADIUS



Resilient RADIUS vs FreeRADIUS



Resilient RADIUS vs FreeRADIUS

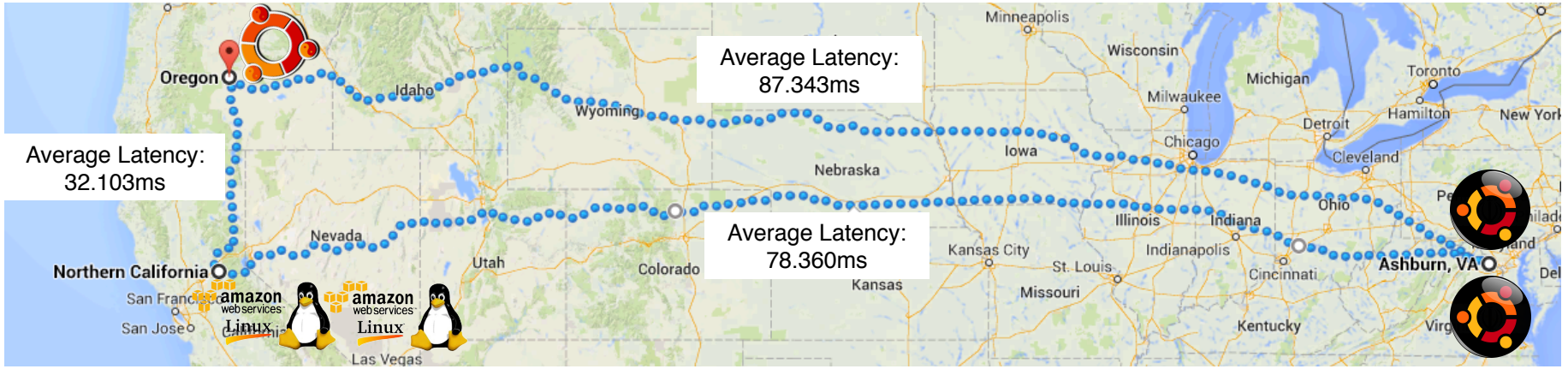
Fail-stop (crash) and
Byzantine faults

Attack	FreeRADIUS	RADIUS Rep	RADIUS Gw
Fail-stop	9s delay	No delay	9s delay
Byzantine	Max delay of 9s	No delay	Up to 9s delay

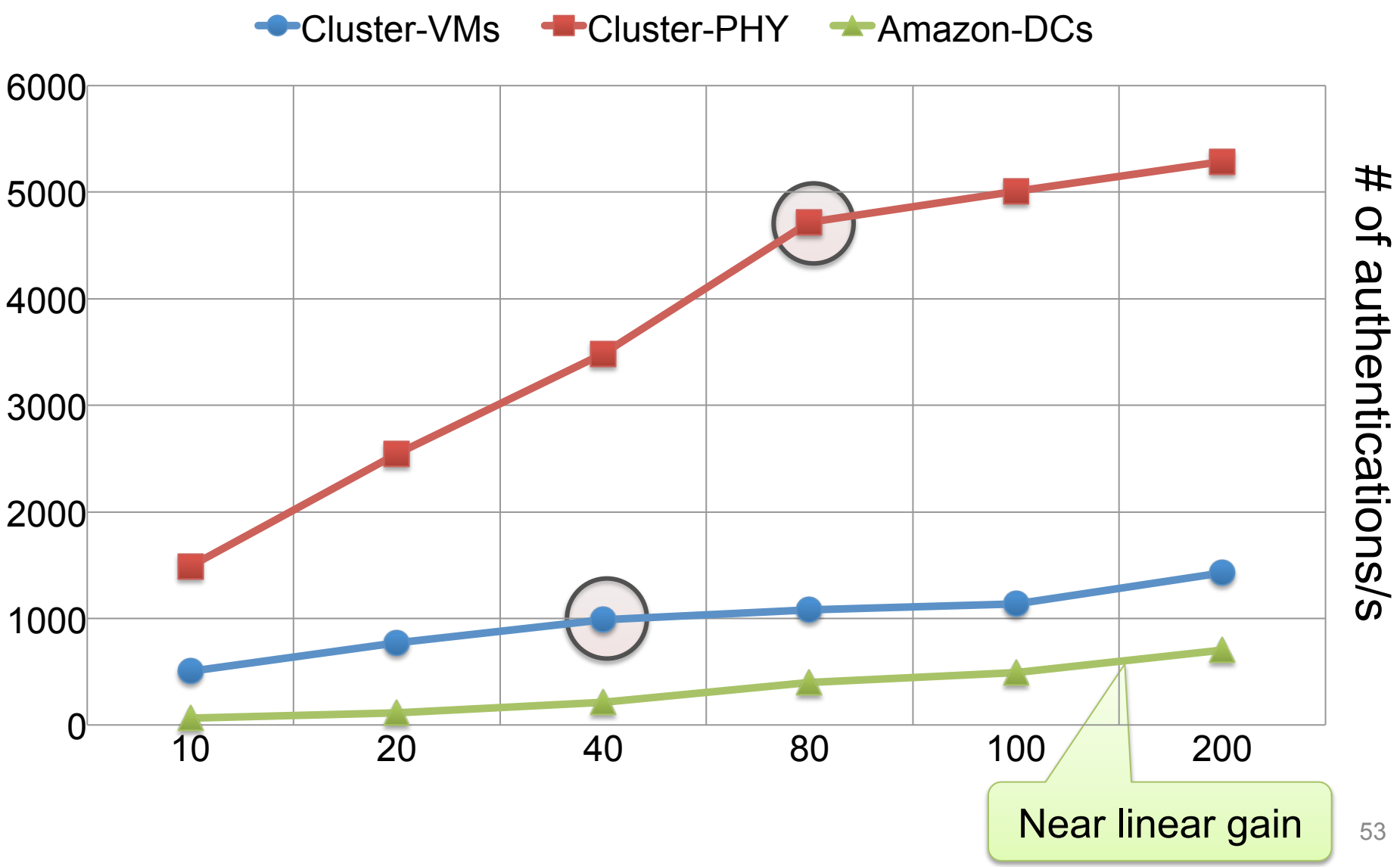
Note: *using the default configuration of the RADIUS protocol, i.e., 3s between each retry.*

Resilient OpenID

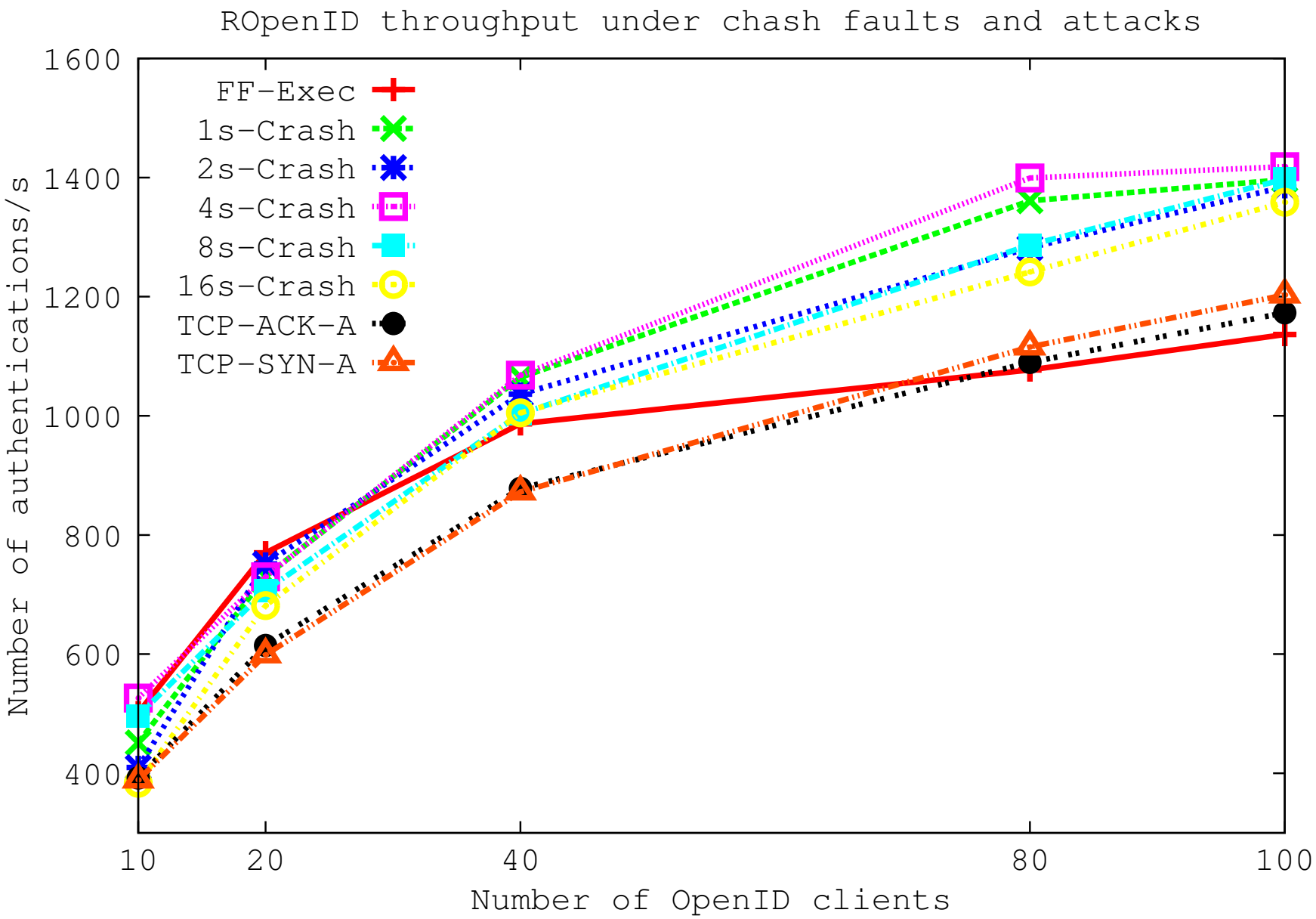
Environment	vCPU	ECUs	MEM	Network
Cluster-VMsR	3	---	4GB	Gigabit Ethernet
Cluster-VMsG	6	---	8GB	Gigabit Ethernet
Cluster-PHY	16	---	32GB	Gigabit Ethernet
Amazon-DCs	2	6.5	7.5GB	Public WAN



Resilient OpenID



Resilient OpenID (faults & attacks)



Outline

Goals & Challenges

Our Solution

Intrusion-Tolerant AAIs

Evaluation

Conclusion

A hybrid architecture for intrusion-tolerant AAIs

A hybrid architecture for intrusion-tolerant AAIs

A new trusted component for ensuring the confidentiality

A hybrid architecture for intrusion-tolerant AAIs

A new trusted component for ensuring the confidentiality

Backward compatibility for both RADIUS & OpenID

A hybrid architecture for intrusion-tolerant AAIs

A new trusted component for ensuring the confidentiality

Backward compatibility for both RADIUS & OpenID

Performance assessment and evaluation under fault & attacks